Symantec Gateway Security Appliance

Installation and Configuration Guide

February 19, 2002

Models 5110, 5200 and 5300

Part Number: 16-30-00030

The software described in this book is furnished under a license agreement and may be used only in accordance with the terms of the agreement.

Copyright notice

Copyright © 1998–2002 Symantec Corporation.

All Rights Reserved.

Any technical documentation that is made available by Symantec Corporation is the copyrighted work of Symantec Corporation and is owned by Symantec Corporation.

Portions copyright (c) eHelp Corporation. All rights reserved.

No warranty

The technical documentation is being delivered to you AS-IS and Symantec Corporation makes no warranty as to its accuracy or use. Any use of the technical documentation or the information contained therein is at the risk of the user. Documentation may include technical or other inaccuracies or typographical errors. Symantec reserves the right to make changes without prior notice.

No part of this publication may be copied without the express written permission of Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

Trademarks

Microsoft, MS-DOS, Windows, and Windows NT are registered trademarks of Microsoft Corporation. IBM, OS/2, and OS/2 Warp are registered trademarks of International Business Machines Corporation. Novell and NetWare are registered trademarks of Novell Corporation. 3Com and EtherLink are registered trademarks of 3Com Corporation. Compaq is a registered trademark of Compaq Corporation. Zip and Jaz are registered trademarks of Iomega Corporation. SuperDisk is a trademark of Imation Enterprises Corporation, Rainwall is a registered trademark of Rainfinity Corporation. This product includes software developed by the Apache Software Foundation.

Other product names mentioned in this manual may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.

Technical support

As part of Symantec Security Response, our global technical support group maintains support centers throughout the world. Our primary role is to respond to specific questions on product feature/function, installation, and configuration, as well as to author content for our web-accessible Knowledge Base. We work collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion, such as working with Product Engineering as well as our Security Research Centers to provide Alerting Services and Virus Definition Updates for virus outbreaks and security alerts.

Highlights of our support offerings include:

- A range of support options giving you the flexibility to select the right amount of service for any size organization
- Telephone and Web support components providing rapid response and up-to-the-minute information
- Upgrade Insurance delivering automatic software upgrade protection
- Content Updates for virus definitions and security signatures ensuring the highest level of protection
- Global support from Symantec Security Response experts available 24x7 world wide in a variety of languages
- Advanced features such as the Symantec Alerting Service and Technical Account Manager role offering enhanced response and proactive security support

Please reference our website for current information on Support Programs. The specific features available may vary based on the level of support purchased and the specific product you are using.

Registration and licensing

If the product you are implementing requires Registration and/or a License Key, the fastest and easiest way to register your service is to access our licensing and registration site at www.symantec.com/certificate. Alternatively, you may go to http://www.symantec.com/techsupp/ent/enterprise.html, select the product you wish to register and, from the Product Home Page select the Licensing and Registration link.

Contacting support

Customers with a current support agreement may contact the Technical Support team via phone or web at www.symantec.com/techsupp.

When contacting support, please be sure to have the following information available:

- Product Release Level
- Hardware Information

  Available memory, Disk Space, NIC information
- Operating System

  Version and Patch Level
- Network Topology

  Router, Gateway and IP Address information
- Problem Description
  - Error Messages/Log Files
  - Troubleshooting performed prior to contacting Symantec
  - Recent software configuration changes and/or network changes

Customer service

Contact Enterprise Customer Service online at http://www.symantec.com, select the appropriate Global Site for your country, then chose 'Service and Support'. Customer Service is available to assist with the following types of issues:

- Questions regarding product licensing or serialization
- Update product registration with address or name changes
- General product information (eg. features, language availability, dealers in your area)
- Latest information on product updates and upgrades
- Information on upgrade insurance and maintenance contracts
- Information on Symantec Value License Program
- Advise on Symantec's technical support options
- Non-technical presales questions
- Missing or defective CD-ROMs or manuals

Contents

1 Product Overview

Firewall 1-8
VPN 1-9
Intrusion Detection System (IDS) 1-9
Antivirus scanning 1-10
Content filtering 1-11
High availability/load balancing 1-12
Symantec Raptor Management Console 1-12
Appliance models and specifications 1-13
Model 5110 1-13
Model 5200 1-14
Model 5300 1-14
Components list 1-15
Documentation 1-16
Checking the hardware 1-17

2 Installation

Cautions and warnings 2-19
Stand-alone hardware installation 2-20
Rack-mount instructions 2-22
Back panel of model 5110 2-24
Connect model 5110 to the network 2-25
Connect power cord to model 5110 2-25
Power on the model 5110 2-26
Back panel of models 5200 and 5300 2-26
Connect models 5200 and 5300 to the network 2-27
Connect the power cord to models 5200 and 5300 2-27
Power on the models 5200 and 5300 2-28
Connect an Uninterruptible Power Supply (UPS) 2-28

3 Initial Setup

Front panel layout - model 5110 3-30
Front panel layout - models 5200 and 5300 3-32
Front panel controls 3-34
Network address information 3-35
Network configuration worksheet 3-36
Initial network configuration procedure 3-38
Display system information 3-42
Use the system menu 3-43
Get your license key 3-45
Restoring the Symantec Gateway Security appliance operating system 3-46
Install SRMC 3-48
Connect to Symantec Gateway Security appliance 3-54
Setup wizard 3-56

4 Firewall

QuickStart wizard 4-64
    Quickstart firewall configuration results 4-68
SMTP Wizard 4-70

5 VPN

Configure S2S tunnels using the wizard 5-79
Configure VPN Client tunnels using the wizard 5-95

6 Routes and DNS

Setting up routes 6-100
    Specifying the default gateway 6-101
    Creating static routes 6-102
Configure the DNS proxy 6-104
    Provide private DNS file address statements 6-104
    Provide hosts.pub file information 6-107
Verify connectivity 6-108

7 Management Console

Monitor Symantec Gateway Security appliance 7-112
Managing passwords 7-114
Remote management password 7-114
Root and secure remote login passwords 7-116
Change system settings 7-117
Change the date and time 7-118
Define a license key 7-119
Perform a system shutdown from SRMC 7-121
Perform a system reboot from SRMC 7-121
Back up configuration files 7-122
Restore configuration files 7-124
Apply patches to the Symantec Gateway Security software 7-126
Manage log files 7-127
Add SRMCs 7-127
Use secure remote login 7-128
Front panel keypad locking 7-129
Use a locked keypad 7-130

8 Intrusion Detection System (IDS)

IDS Components folder 8-132
Configuration 8-132
Reports 8-132
Monitoring 8-133
Configuring the IDS component 8-133
Configuring IDS Signatures 8-134
Using LiveUpdate to update attack signatures 8-139
Viewing IDS Alerts in the IDS Alerts Viewer 8-142
Updating the View in the IDS Alerts Viewer 8-144
IDS Reports 8-145
Configuration Report 8-145
Executive Summary 8-145
IDS notifications 8-147
Blacklist notifications 8-150
Client Program notification 8-152

Mail notifications 8-153
Page notifications 8-155
SNMP notifications 8-157

9 Antivirus Scanning

About Symantec AntiVirus 9-162
Virus detection 9-163
Antivirus scanning on the Symantec Gateway Security appliance 9-165
Configuring antivirus scanning 9-165
Local versus remote scanning 9-166
Configuring the antivirus scan server 9-168
Updating virus definitions 9-171
Running LiveUpdate on demand 9-171
Scheduling LiveUpdate to run automatically 9-173
Configuring proxy services for antivirus scanning 9-173
Configuring antivirus scanning for the FTP and HTTP proxies 9-174
Configuring antivirus scanning for the SMTP proxy 9-178
Enabling antivirus scanning in a rule 9-183
Using the mail filter options 9-186
Filtering mail by attachment file name 9-186
Filtering mail by attachment file size 9-189
Filtering mail by subject 9-191
Filtering mail by domain 9-193
Filtering mail by maximum mail size 9-195
Rejecting invalid mail messages 9-196
Customizing virus messages 9-197

10 Content Filtering

Using content profiles 10-202
Creating rating rule profiles 10-202
Using a ratings profile in a rule 10-204
Searching capabilities 10-205
Customizing WebNOT ratings lists 10-206
Using content restrictions 10-207
Allowing extensions 10-207

Allowing URLs 10-208
HTTP restrictions in a rule 10-209
HTTP URL patterns 10-210
Denying MIME types 10-211

11 High Availability and Load Balancing

About the cluster wizard 11-214
Preparing to create a cluster 11-215
Creating a cluster for software high availability/load balancing 11-215
Creating a cluster for appliance file propagation or hardware HA/LB 11-222
Verifying a cluster 11-224
Modifying a cluster 11-225
Deleting a cluster 11-228
Viewing Cluster Properties 11-229
Propagating appliance configuration files 11-230
HA/LB Implementation 11-232
Three appliance cluster example 11-233
Setting Up VIPs 11-236
HA/LB terms 11-240

A Important safeguards

B IDS and antivirus scanning log messages

IDS Messages B-246
IDS Informational Messages B-247
IDS Alerts B-252
Antivirus scanning messages B-255

C Licenses

GNU GENERAL PUBLIC LICENSE C-262
NO WARRANTY C-266
SYMANTEC APPLIANCE LICENSE AND WARRANTY AGREEMENT C-267
1. Software License: C-267
2. Content Updates: C-268
3. Limited Warranty: C-268

4. Disclaimer of Damages: C-270
5. U.S. Government Restricted Rights: C-271
6. Export Regulation: C-271
7. General: C-271
8. Excluded Software: C-272

D Serial Port Cable

Serial 9-Pin Cable Specifications D-273

Index

Chapter 1

Product Overview

The Symantec Gateway Security appliance integrates core Symantec technologies into a unique, integrated solution to effectively prevent security breaches at the perimeter. The appliance combines mature firewall, antivirus, intrusion detection, content filtering, and virtual private network (VPN) capabilities in a single, ready-to-deploy system.

All functions are managed by a common console and utilize a common reporting structure for easy-to-understand data collection. The Symantec Gateway Security appliance provides network security at the gateway between the Internet and a corporate network or between network segments. Using the Symantec Raptor Management Console (SRMC), all functions can be configured and managed either locally or remotely. The Symantec Gateway Security appliance provides all of the network security you need in one appliance that is easy to install, configure, and operate.

The Symantec Gateway Security appliance maximizes the security of your network without compromising performance. It provides you with the ability to easily manage your network security and make modifications as your security needs evolve.

The Symantec Gateway Security appliance is a unique security solution that combines technologies from the Symantec Enterprise Firewall, Symantec Enterprise VPN, intrusion detection, content filtering, and antivirus scanning in one appliance.

Firewall

The Symantec Gateway Security appliance includes technologies from Symantec's Enterprise Firewall technology to protect enterprise assets and business transactions with one of the most secure, high-performance solutions for ensuring safe connections with the Internet and between networks. Its unique architecture delivers security and speed, providing strong and transparent firewall protection against unwanted intrusion without slowing the flow of approved traffic on enterprise networks. Features include:

- Standard Proxies

  These proxies handle common services, such as telnet, HTTP, FTP, RealAudio, and others. Standard proxies offer the highest level of logging and ease of use.

  Unless specifically stated otherwise, when this manual describes how traffic is passed, it does so using standard proxies.

- Custom Protocols

  You can use the Symantec Raptor Management Console (SRMC) Protocol Properties page to configure generic services provided by the hosts residing on either side of the gateway. Custom or "generic" services include any service not supported by one of the Symantec Gateway Security appliance's proxy server applications.

- Address Transforms

  Address Transforms give you the ability to control addressing, letting you present routable addresses for connections passing through a system interface or secure tunnel. This helps you to route connections to the correct destination when your site has addressing overlap issues or other routing problems.

- Configuration Reports

  You can generate and print full reports for every configurable item of the Symantec Gateway Security appliance.

- Defense Against Denial of Service Attacks

  A denial of service attack prevents legitimate users from accessing Internet services by consuming network resources with an onslaught of continuous service requests. You can configure your Symantec Gateway Security appliance to quickly recognize this type of attack and immediately drop all packets coming from a hostile source.

See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for more information.

VPN

The Symantec Gateway Security appliance includes technology from the Symantec Enterprise VPN Server, which allows organizations to securely extend their network perimeters beyond the enterprise firewall by providing VPN server proxy-secured scanning and personal firewall protection via the Symantec Enterprise VPN client. A completely integrated and standards-based solution, it allows organizations to establish safe, fast, and inexpensive connections, enabling new forms of business and secure access to information for authorized partners, customers, telecommuters, and remote offices.

The Symantec Gateway Security appliance uses VPN tunnels to send encrypted and encapsulated IP packets over public networks securely to another VPN server. Symantec's IPsec-compliant Symantec Enterprise (SEVPN) VPN Client 7.0 is optional and available with the full VPN function cross grade license.

VPN features include:

- VPN Policies

  The Symantec Gateway Security appliance ships with pre-configured general VPN policies which you can apply to your secure tunnels.

  For example, there are IPsec/IKE policies and IPsec/Static policies. You can apply these policies to each IKE or IPsec/Static secure tunnel you create.

- Support for third party IKE clients

  Symantec Gateway Security supports scalable policy management for any IKE-compliant, third party mobile client through tunnels based on users and user groups.

See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for more information.

Intrusion Detection System (IDS)

The Symantec Gateway Security appliance provides network-based intrusion detection technology designed to fortify your organization's perimeter defenses; it transparently monitors traffic on the network to prevent security violations and to protect in-house resources. The Intrusion Detection System (IDS) technology monitors network traffic for suspicious behavior and responds to intrusion attacks in real time. Features include:

- Detection of attacks

  Detect atomic network-based attacks and report the alerts to the SRMC. The atomic signatures detect many widespread attacks including Teardrop,

Whisker, Girlfriend, NOOP, buffer overflow, and various attacks specific to various operating systems (Windows, Solaris, Linux, etc.) and applications/services (HTTP, DNS, etc.).

Respond to network attacks with pre-configured actions such as dropping attack packets.

- Separate IDS monitoring, configuration, and reports views

  View and respond to attack alerts in real time using the IDS Alerts Viewer and the notifications feature.

  Configure signatures to be on or off, and gated or not gated.

  Generate configuration and Executive Summary reports.
- LiveUpdate of attack signatures

Antivirus scanning

The Symantec Gateway Security appliance provides advanced, high-performance virus scanning and repair. The Symantec Gateway Security appliance features include award-winning antivirus technologies that make Symantec an industry leader in virus protection software. Symantec AntiVirus technology is one of the fastest, most effective virus solutions available for detecting and preventing malicious virus attacks. The Symantec Gateway Security appliance detects malicious viruses, worms, and Trojan horses in all major file types, including mobile code and compressed file formats. Virus definitions and engines are updated automatically via Symantec's LiveUpdate technology, with no interruption in virus scanning. The antivirus technology of the Symantec Gateway Security appliance is scalable, high performing, and reliable.

Features include:

- E-mail (SMTP), Web (HTTP), and FTP traffic scanning
- Configuration options for handling infected files
- Trusted, industry-recognized Symantec AntiVirus core technologies, including:
  - NAVEX (Norton AntiVirus Extensible Engine) allows virus definition AND engine updates without interruption in service or restart of server(s).
  - Bloodhound provides heuristic detection of new and unknown viruses, for more comprehensive protection.
  - LiveUpdate provides automated or manual updates for virus definitions and engines to ensure that protection remains current against newly identified threats.

  - Striker identifies polymorphic computer viruses, which can be some of the most complex and difficult to detect.
- Policy object for scanning of e-mail to optionally block messages by subject line text, message origin, attachment file name or size, attachment type, and overall message size for greater protection against rapidly spreading e-mail-born viruses
- Optional updating of e-mail messages when an infected attachment is repaired or deleted to warn recipients that a virus has been detected

Content filtering

The Symantec Gateway Security appliance provides flexible internet content filtering technology. This increases worker productivity and preserves valuable bandwidth by focusing web access on business related content. At the same time, it decreases exposure to liability by restricting access to potentially objectionable content. URL filtering can be configured on a global, per user, per user group, per IP or per IP group basis.

Features include:

- Internet access permissions based on rules and policies
- URL override to permit access to sites that are blocked by the master database
- Logs and reports

  Logs can be exported to ASCII and .csv formats for representation in popular reporting tools such as WebTrends.
- Comprehensive alerting

  E-Mail, SNMP, Pager, Audio and custom alerts can be configured to notify administrators of policy breaches when users access web content against their organization's policy.
- Access scheduling

  Access to web content can be scheduled by time of day and day of week, maximizing flexibility.
- Transparent operation

  No browser modification is required in client computers.
- Regularly updated URL lists

High availability/load balancing

The Symantec Gateway Security appliance provides high availability and load balancing technology for clustered appliances. In today's business environment, internet access is mission critical. In order to achieve the availability needed while also maximizing your throughput, your security gateways need high availability and load balancing. This new integrated offering ensures easier setup, better performance, and higher security than other high availability/load balancing solutions on the market.

When two or more Symantec Gateway Security appliances are available, the failure of one appliance causes the other appliance to automatically pickup the workload of the failed appliance.

Symantec Raptor Management Console

The Symantec Raptor Management Console (SRMC) is the graphical user interface for managing and monitoring all functions on the Symantec Gateway Security appliance.

Appliance models and specifications

Model 5110

- 50 node license
- Four 10/100Base-T ethernet network interfaces
- Serial console interface
- Serial port for uninterruptible power supply (UPS)
- LCD display and keypad for easy set-up
- Six status indicator LEDs

Figure 1-1 Symantec Gateway Security appliance Model 5110

Note: Symantec Security Gateway appliance ships with either High Encryption (3DES/AES) or DES encryption.

Table 1-1 Model 5110 specifications

Parameter	Specification
Dimensions	17.00 x 12.50 x 1.75 inches (43.2 x 31.8 x 4.5 cm) Fits a standard 19" equipment rack; single rack unit height
Weight	9 lbs 3 oz. (4.2 kg)
Network interfaces	Four 10/100Base-T ethernet connections
User interface	2 x 16 liquid crystal display on front panel LEDs: transmit/receive, link, collision, 100 M, disk activity, temperature
Operating environment	32° to 108° F (0° to 40° C) 10% to 90% humidity (non-condensing)

Parameter	Specification
Power requirements	Input rating 100-240V, 50/60Hz
Maximum power consumption	50 watts

Model 5200

- 250 node license
- Four 10/100Base-T ethernet network interfaces
- Serial console interface
- Serial port for uninterruptible power supply (UPS)
- LCD display and keypad for easy set-up
- Six status indicator LEDs

Model 5300

- Unlimited node license
- Four 10/100Base-T ethernet network interfaces
- Serial console interface
- Serial port for uninterruptible power supply (UPS)
- LCD display and keypad for easy set-up
- Six status indicator LEDs

Figure 1-2 Symantec Gateway Security appliance Model 5300

Table 1-2 Models 5200 and 5300 specifications

Parameter	Specification
Dimensions	17.50 in. x 22.75 in. x 1.75 in (44.5 cm x57.8 cm x 4.5 cm) Fits a standard 19" equipment rack; single rack unit height
Weight	20 lbs (9 kg)
Network interfaces	Four 10/100Base-T ethernet connections
User interface	2 x 16 liquid crystal display on front panel LEDs: transmit/receive (2), link (2), disk activity (1), temperature
Operating environment	32° to 95° F (0° to 35° C) 10% to 90% humidity (non-condensing)
Power requirements	Input rating 100-240V, 50/60Hz
Maximum power consumption	100 watts (typical), 130 watts (max)

Components list

The Symantec Gateway Security appliance ships with the components listed in the following table.

Table 1-3 Components list

Part	Description
Symantec Gateway Security appliance	A single device, rack-mount or stand-alone
Five rubber feet	For resting the appliance on a flat surface **Note:** Models 5200 and 5300 do not come with rubber feet.
Rack-mount brackets	Hardware for rack-mounting the appliance

Part	Description
Software CD-ROM containing:	• SRMC Management Console (GUI) • Restore Image • Adobe Acrobat Reader® The following documentation in PDF format: • *Symantec Gateway Security Appliance Installation and Configuration Guide* (this book) • Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide • Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide • Quick Start Card
License Key and Support Request form	A form which provides the license serial number and directions on how to obtain the license key and register for 1 year of Gold support. This form also contains the license for the appliance.
Power cord	A power cord required for the country in which the appliance will operate. Available country cord types are: Australia, Euro, UK, and USA.
Printed documentation	• Symantec Gateway Security Appliance Installation and Configuration Guide • Quick Start Card • Release Notes

Documentation

The Symantec Gateway Security appliance functionality is described in three manuals:

- *The Symantec Gateway Security Appliance Installation and Configuration Guide* (this book)

  This guide covers all the functionality of the Symantec Gateway Security appliance except firewall and VPN features.
- Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide

This guide covers topics related to the firewall and VPN features, including: base components, access controls, secure tunnels, VPN policies, remote policies, and monitoring controls. It is provided in PDF format on the Symantec Gateway Security appliance Software CD-ROM.

- Symantec Enterprise Firewall, Symantec Enterprise VPN, and VelociRaptor Firewall Appliance Reference Guide

  This guide provides advanced technical information about network security and advanced configuration examples.

You will need to use all these manuals to fully configure and manage the Symantec Gateway Security appliance.

Checking the hardware

After carefully unpacking the Symantec Gateway Security appliance, compare the actual kit contents with **Table 1-3** to ensure that you have received all ordered components. Follow the instructions on the Quick Start Card to install and set up the appliance.

Chapter 2

Installation

This chapter describes the following procedures:

- Installing the Symantec Gateway Security appliance models (5110, 5200 and 5300) as a rack-mounted component or as a stand-alone device
- Connecting the Symantec Gateway Security appliance to your network
- Performing the initial setup of your Symantec Gateway Security appliance

---

Note: Installation procedures differ for Symantec Gateway Security appliance model 5110, and the 5200 and 5300 models, due to the different layouts of their front and back panels.

Cautions and warnings

Because this is an electrically powered device, adhere to the listed warnings and cautions when installing or working with the Symantec Gateway Security appliance.

Warning: Read the installation instructions before connecting the system to its power source.

Note: Refer to Important safeguards on page 243 for information regarding the setup and placement of the Symantec Gateway Security appliance.

Stand-alone hardware installation

The Symantec Gateway Security appliance model 5110 ships with five rubber feet for use when the appliance is set up as a freestanding unit.

Note: Models 5200 and 5300 do not come with rubber feet.

To install the Symantec Gateway Security appliance as a stand-alone device

1. Make sure that the installation site has a smooth and level surface, such as the top of a computer table. Also, avoid placing the Symantec Gateway Security appliance in an area with a lot of clutter, such as books or other hardware devices.
2. Attach the rubber feet to the five indentations on the bottom of the appliance. See Figure 2-1.

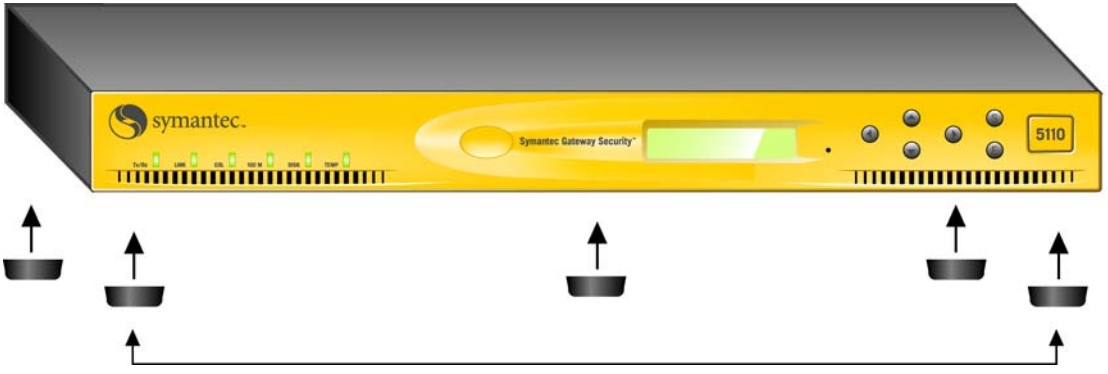


Figure 2-1 Freestanding Model 5110 with rubber feet

3. Place the unit in a secure location away from foot traffic. The installation site must meet minimum environmental specifications as described in Table 1-1.
4. Check that the power source is adequate for the Symantec Gateway Security appliance and that the outlet is located within reach of the supplied power

cord without stretching or putting strain on the cord. Refer to **Connect model 5110 to the network on page 25** or **Connect models 5200 and 5300 to the network on page 27** for details on attaching signal cables.

Caution: Do not use an extension cord to supply power to this unit.

---

5 After cabling the unit into the network, properly dress the cables and position them away from foot traffic to avoid a potential tripping hazard.

Rack-mount instructions

The following rack-mount instructions apply to all appliance models.

Note: Because rack hardware can differ from site to site, the screws shipped with the unit may not be of the proper thread size for your needs. Before proceeding, obtain screws of the proper size and length for your rack installation if necessary.

To mount the appliance in a standard 19-inch equipment rack

1 Connect the mounting brackets to the sides of the appliance towards the front or the rear of the case. See Figure 2-2.

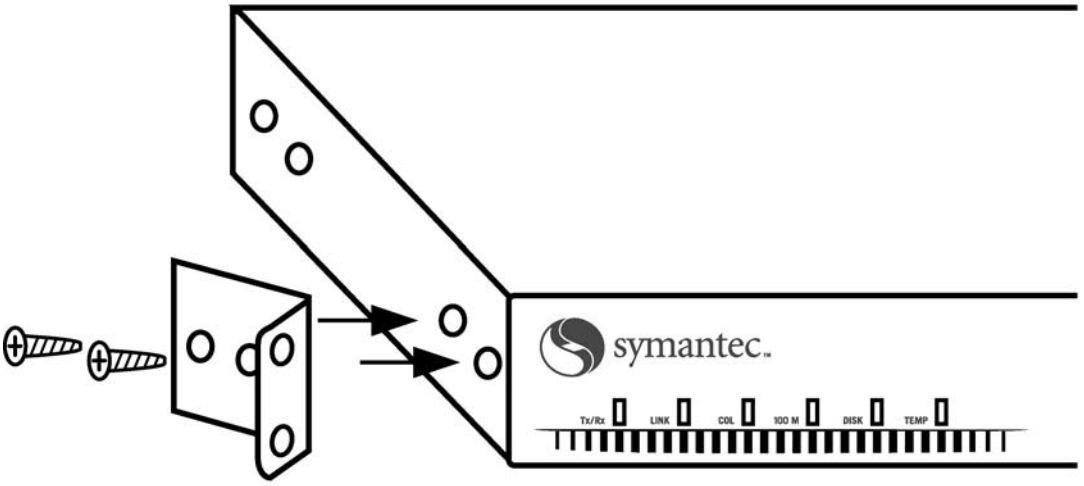


Figure 2-2 Rack-mount bracket installation

2 Secure the mounting brackets to the equipment rack. See Figure 2-3 or Figure 2-4.

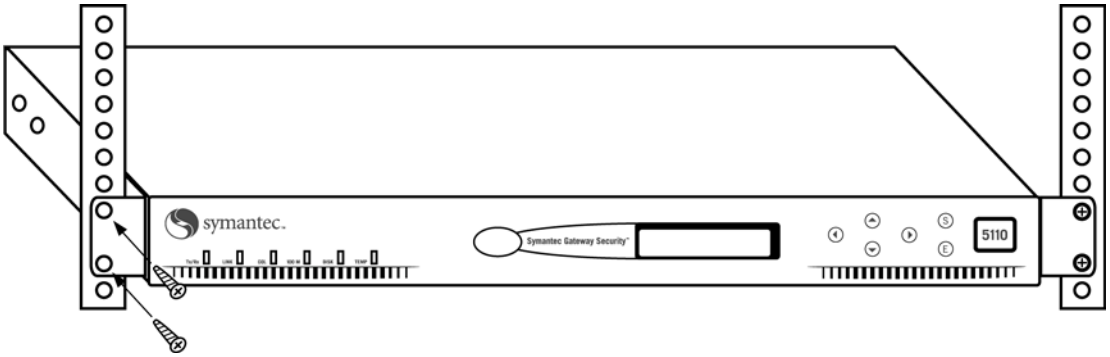


Figure 2-3 Rack-mount rack installation - front

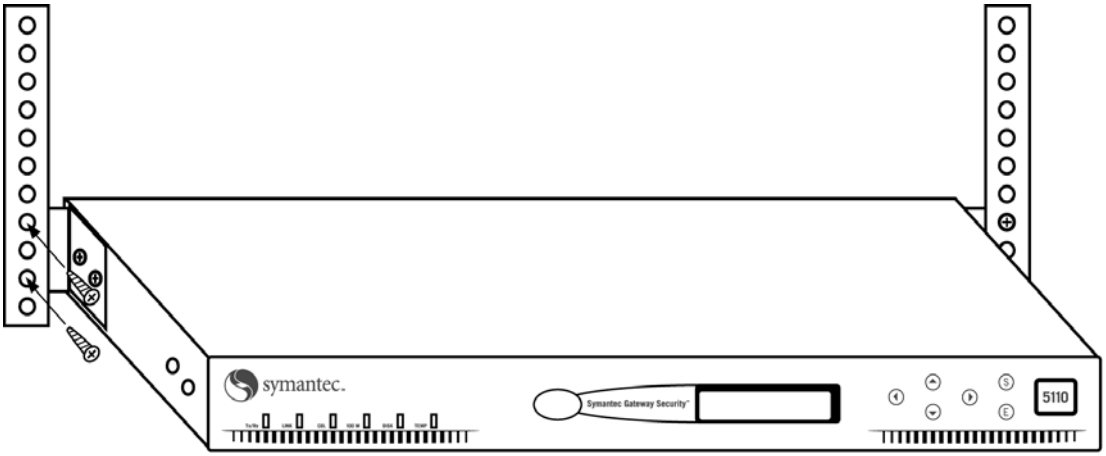


Figure 2-4 Rack-mount rack installation - back

Back panel of model 5110

This section describes the features of the back panel of the Symantec Gateway Security appliance model 5110.

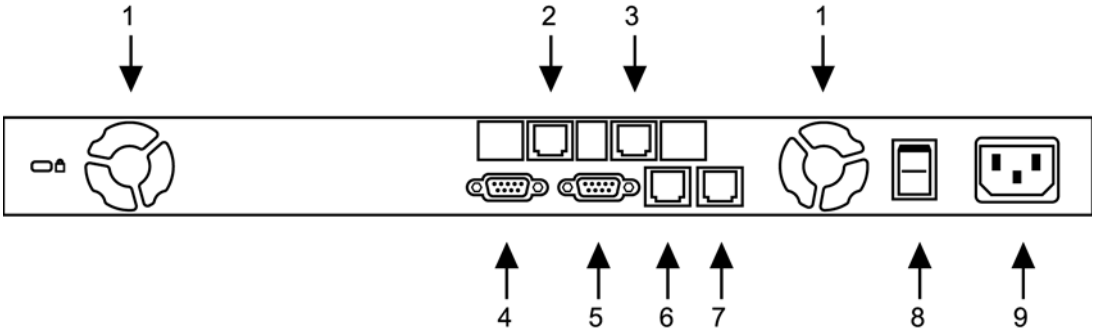


Figure 2-5 Model 5110 back panel

Table 2-1 Model 5110 back panel

Back panel location	Description
1	The **Cooling fans** maintain a proper operating temperature. Ensure that the ventilation holes in the front and back are not blocked.
2	**Auxiliary 2** network connectors enable Ethernet network connections and accept the 10/100Base-T network cables.
3	**Auxiliary 1** network connectors enable Ethernet network connections and accept the 10/100Base-T network cables.
4	The **Serial console** port (155200 Bps) allows you to connect a terminal emulator to act as a system console. This lets you logon to the system console and access the appliance Linux OS locally. For serial cable specifications see **Serial 9-Pin Cable Specifications on page 273**.
5	The **Serial connector** allows you to connect a UPS to the serial port for smart UPS support (See **Connect an Uninterruptible Power Supply (UPS) on page 28**).
6	**Outside** Network connection (eth 1) enable Ethernet network connections and accept the 10/100Base-T network cables.

Table 2-1 Model 5110 back panel

Back panel location	Description
7	**Inside** Network connection (eth 0) enable Ethernet network connections and accept the 10/100Base-T network cables.
8	The **Power switch** toggles the power on or off.
9	The **Power socket** receives the AC cord that is provided.

Connect model 5110 to the network

The Symantec Gateway Security appliance model 5110 back panel provides a total of four ethernet connections. Your network connection requirements may differ depending on your site's configuration. Refer to **Figure 2-5** for the connection instructions below.

To connect your network

1. Plug the RJ-45 connector from the Internet into the Outside network connection (**6**).
2. Plug the RJ-45 connector from the LAN into the Inside network connection (**7**).
3. Plug the RJ-45 connector from any other service network (if present) into the Aux 1 network connection (**3**).
4. Plug the RJ-45 connector from any other service network (if present) into the Aux 2 network connection (**2**).

Connect power cord to model 5110

To connect power to the appliance model 5110

1. Plug the power cord into the appropriate connector on the rear panel (**9**).
2. Connect the power supply cord from the appliance to an electrical outlet or UPS supply unit.

For UPS configuration details, see **Connect an Uninterruptible Power Supply (UPS) on page 28**.

Power on the model 5110

Turn on the power by pressing the **On/Off** switch on the back of the Symantec Gateway Security appliance.

- The hard disk spins up, the fans turn on, and the LCD screen lights up.
- A number of status messages are displayed on the LCD screen as the appliance completes its boot process.

Back panel of models 5200 and 5300

This section describes the features of the back panel of the Symantec Gateway Security appliance models 5200 and 5300.

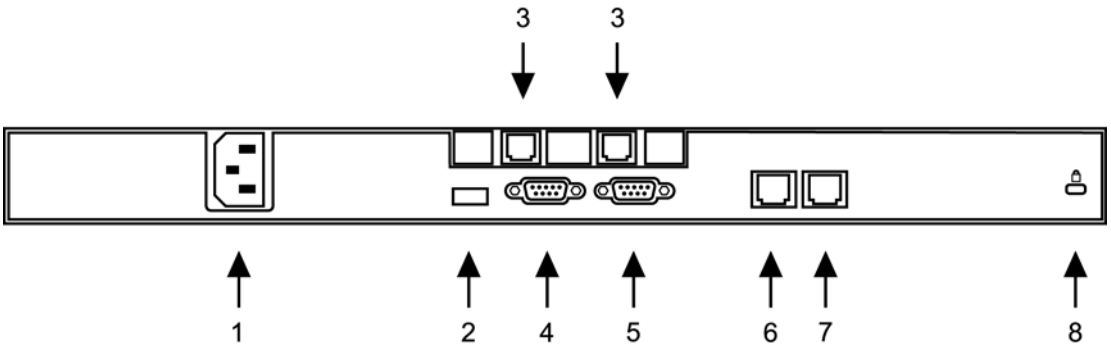


Figure 2-6 Models 5200 and 5300 back panel

Table 2-2 Models 5200 and 5300 back panel

Back panel location	Description
1	The **Power socket** receives the AC cord that is provided.
2	The **USB port** is not currently supported.
3	**Auxiliary 1 and Auxiliary 2** network connectors enable Ethernet network connections and accept the 10/100Base-T network cables.
4	The **Serial connector** allows you to connect a UPS to the serial port for smart UPS support. See **Connect an Uninterruptible Power Supply (UPS) on page 28**.

Table 2-2 Models 5200 and 5300 back panel

Back panel location	Description
5	The **Serial console** port (155200 Bps) allows you to connect a terminal emulator to act as a system console. This lets you logon to the system console and access the appliance Linux OS locally. For serial cable specifications see Serial 9-Pin Cable Specifications on page 273.
6	**Outside** Network connection (eth 1) enable Ethernet network connections and accept the 10/100Base-T network cables.
7	**Inside** Network connection (eth 0) enable Ethernet network connections and accept the 10/100Base-T network cables.
8	The **Security lock hole** is used to lock the unit to a secure location.

Connect models 5200 and 5300 to the network

The Symantec Gateway Security appliance models 5200 and 5300 back panel provide a total of four ethernet connections. Your network connection requirements may differ depending on your site's configuration. Refer to Figure 2-6 for the connection instructions below:

1. Plug the RJ-45 connector from the Internet into the Outside network connection (**6**).
2. Plug the RJ-45 connector from the LAN into the Inside network connection (**7**).
3. Plug the RJ-45 connector from any other service network (if present) into the Aux 1 network connection (**3**).
4. Plug the RJ-45 connector from any other service network (if present) into the Aux 2 network connection (**3**).

Connect the power cord to models 5200 and 5300

To connect power to appliance models 5200 and 5300

1. Plug the power cord into the appropriate connector on the rear panel (**1**).
2. Connect the power supply cord from the appliance to an electrical outlet or UPS supply unit.

For UPS configuration details, see **Connect an Uninterruptible Power Supply (UPS) on page 28**.

Power on the models 5200 and 5300

Turn on the power by pressing the **On/Off** button on the front of the Symantec Gateway Security appliance models 5200 and 5300.

- The hard disk spins up, the fans turn on, and the LCD screen lights up.
- A number of status messages are displayed on the LCD screen as the appliance completes its boot process.

Connect an Uninterruptible Power Supply (UPS)

When the Symantec Gateway Security appliance is configured to use an uninterruptible power supply (UPS), the appliance can power down in an orderly manner in the event of a power failure. The appliance communicates directly to the UPS unit through the serial port.

The recommended supplier for UPS units is American Power Conversion (www.apcc.com).

To configure Symantec Gateway Security for UPS support, you must first connect the appliance to the UPS through a serial port as follows:

1. Plug the UPS into the wall socket.
2. Turn on the UPS.
3. Plug the Symantec Gateway Security appliance into the UPS power socket.
4. Connect the UPS serial cable to the UPS unit and the Symantec Gateway Security appliance.

   Refer to **Figure 2-5** for the location of the UPS port (**5**) on the model 5110 back panel.

   Refer to **Figure 2-6** for the location of the UPS port (**4**) on the models 5200 and 5300 back panel.

Note: To configure UPS support on the Symantec Gateway Security appliance, access the System Menu, as described in **Use the system menu on page 43**. You can also turn UPS support on from the SRMC Symantec Gateway Security Setup wizard, which is detailed in **Setup wizard on page 56**.

Chapter 3

Initial Setup

This chapter describes the procedures for configuring the Symantec Gateway Security appliance network parameters for use with the Symantec Raptor Management Console (SRMC), installing the SRMC, connecting the SRMC to the appliance, and running the Setup Wizard. This chapter also describes the various Symantec Gateway Security appliance hardware features.

Symantec Gateway Security appliance has an integral LCD display located on the front of the unit. Using the appropriate buttons, you can enter basic configuration information into the Symantec Gateway Security appliance, as well as monitor certain system operating parameters.

Front panel layout - model 5110

The Symantec Gateway Security appliance model 5110 front panel, as shown in Figure 3-1, contains six data entry and navigation keys and a two line x 16 character liquid crystal display area. The initial configuration of the Symantec Gateway Security appliance takes place at the unit's front panel, where you enter and modify parameters such as system and network IP addresses.

Figure 3-1 Symantec Gateway Security appliance model 5110 front panel

Table 3-1 Model 5110 front panel descriptions

Front panel locations	Description
1	The **Status Indicators** signal Ethernet and hard drive activity: • **Tx/Rx** (Transmit/Receive) blinks when there is network traffic on the inside interface. • **Link** indicates an active network connection on the inside interface. • **Col** blinks when a collision is detected on the inside interface. • **100 M** indicates that 100 BaseT ethernet is being used on the inside interface. • **Disk** indicates hard disk activity on the hard disk drive.
2	The **Temp** indicator blinks to indicate temperature status, blinking slowly for temperature warnings and quickly for temperature failures. If the Symantec Gateway Security appliance is in danger of overheating, a log message is sent to SRMC.

Table 3-1 Model 5110 front panel descriptions

Front panel locations	Description
3	The **LCD screen** displays the Symantec Gateway Security version number and system health monitoring information. The LCD screen is the same on all models. Although relatively small in size, it allows you to monitor appliance status, modify configuration parameters, and re-initialize the appliance. The displays available at the LCD panel are as follows: • System startup self-tests • Performance monitoring • System menu (see **Use the system menu on page 43**) As the appliance boots up, the LCD displays status messages.
4	The factory reset **pinhole**, when pressed, resets the Symantec Gateway Security appliance in the following manner: • Network IP address information is erased. • SRMC workstation connection information is erased. • License information remains intact.
5	The front panel **push buttons** let you enter network information directly into the appliance (see **Front panel controls on page 34**).

Front panel layout - models 5200 and 5300

The Symantec Gateway Security appliance models 5200 and 5300 front panel, as shown in Figure 3-2, contains six data entry and navigation keys and a two line, 16 character liquid crystal display area. The initial configuration of the Symantec Gateway Security appliance takes place at the unit's front panel, where you enter and modify parameters such as system and network IP addresses.

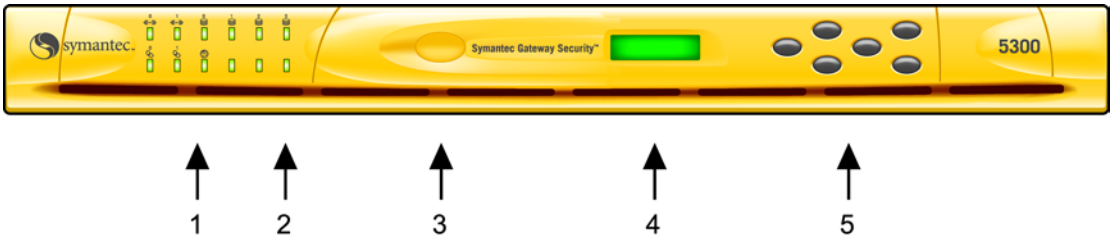


Figure 3-2 Symantec Gateway Security appliance model 5200 and 5300 front panel

Table 3-2 Model 5200 and 5300 front panel descriptions

Front panel locations	Description
1	The **Status Indicators** signal network activity, ethernet connections, and hard disk drive activity. blinks when there is traffic on the network interfaces (labeled 0 for outside and 1 for inside). glows steadily to indicate an active connection on the network interfaces (labeled 0 for outside and 1 for inside). blinks when there is activity on the hard disk drive (labeled 0, 1 through 3 are not used).
2	The **Temp** indicator blinks to indicate temperature status, blinking slowly for temperature warnings and quickly for temperature failures. If the Symantec Gateway Security appliance is in danger of overheating, a log message is sent to SRMC.
3	The **Power** button turns the power to the appliance on and off.

Table 3-2 Model 5200 and 5300 front panel descriptions

Front panel locations	Description
4	The **LCD screen** displays the Symantec Gateway Security appliance version number and system health monitoring information. The LCD screen is the same on all models. It allows you to monitor appliance status, modify configuration parameters, and re-initialize the appliance. The displays available at the LCD panel are as follows: • System startup self-tests • Performance monitoring • System menu (see **Use the system menu on page 43**) As the appliance boots up, the LCD displays status messages.
5	The front panel **push buttons** let you enter network information directly into the appliance (see **Front panel controls on page 34**).

Front panel controls

The front panel controls are the same on all models. Use the following push button instructions to enter all required setup information (detailed in the **Initial network configuration procedure on page 38**) into the Symantec Gateway Security appliance.

Note: The front panel buttons perform dual functions. These functions depend upon whether the appliance is in initial setup mode (see **Initial network configuration procedure on page 38**), or if the system menu has been entered (see **Use the system menu on page 43**). Refer to the bulleted descriptions below.

Up (^) and down (v) arrow buttons:

- During initial setup, use the up (^) and down (v) arrow buttons to enter the IP addresses the appliance prompts you for. These buttons increment and decrement the current number displayed on the LCD. When the first set of numbers is correct, use the (>) arrow button to move to the next set.
- When you enter the System Menu (see **Use the system menu on page 43**), use the up (^) and down (v) arrow buttons to move to the previous menu item (^) or to the next (v) menu item.

Left (<) and right (>) arrow buttons:

- During initial setup, use the left (<) and right (>) arrow buttons to move across the LCD panel.
- When you enter the System Menu (see **Use the system menu on page 43**), use the left and right arrow buttons to move to the previous menu item (<) or to the next (>) menu item.

E (Enter) button:

- During initial setup, when an IP address or other information is complete, press the E button to accept it.
- Press the E button to enter the System Menu when the Symantec Gateway Security appliance is in monitoring mode. From the System Menu, use the E button to accept displayed LCD data.

S (Select) button:

- When you enter the System menu, use the S button to cancel out of a menu item and return to the top menu level.

Network address information

When the appliance boots for the first time, you must enter the network address information for the SRMC that will manage the appliance. Refer to the network configuration in Figure 3-3 for the examples given as part of the address setup instructions in this section.

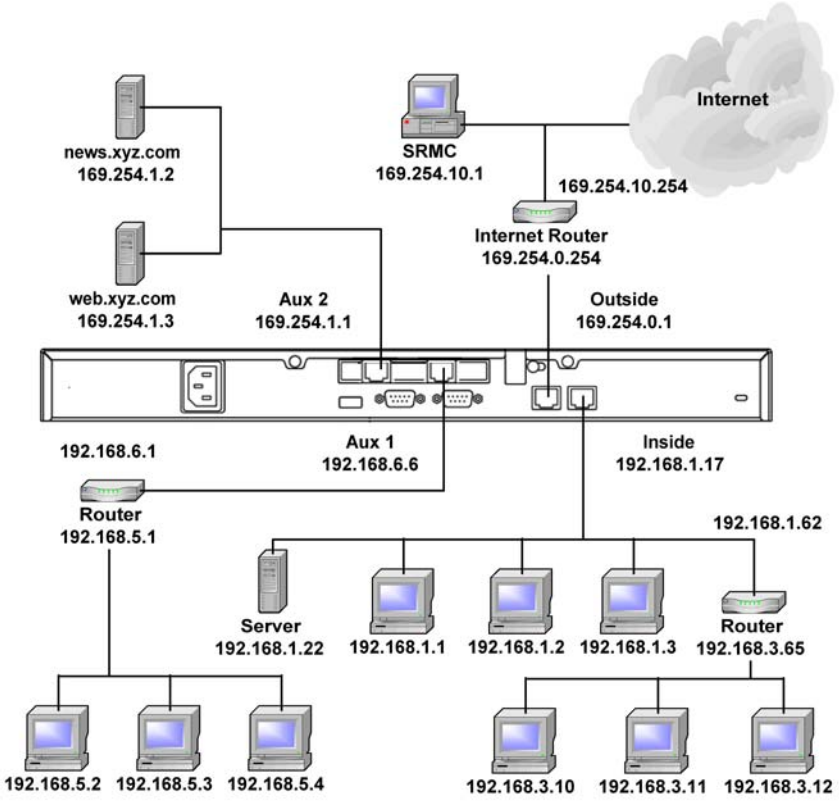


Figure 3-3 Symantec Gateway Security appliance protected network

Network configuration worksheet

During the Symantec Gateway Security appliance setup process, you are prompted to enter network address information. Once those addresses are entered, Symantec Gateway Security's LCD panel displays three passwords that you will need to initiate remote management. Use the worksheet on the next page to make note of the passwords. You can change them once you have set up the SRMC to begin remote management. For details on changing passwords, see **Managing passwords on page 114**.

Store this completed form in a secure location. This form can also serve as a permanent record for each Symantec Gateway Security appliance installed at your site. For details on the worksheet items listed below, see **Initial network configuration procedure on page 38**.

Make a copy of this worksheet to record the output data.

Network configuration worksheet

User input during initial setup:

Interface IP address_____

Netmask _____

Gateway address _____

SRMC address _____

Symantec Gateway Security appliance output during initial setup:

SRMC password[1] _____

SRL (Secure Remote Login) password[1]_____

Root password[1]_____

System ID_____

[1] Passwords are output during the hardware configuration process

Initial network configuration procedure

The Symantec Gateway Security appliance first prompts you to enter the IP address of the network port that will communicate with the SRMC system that will manage the Symantec Gateway Security appliance.

To perform the initial network configuration of an appliance

1. Start the appliance initial setup by pressing the **E** (Enter) button.
2. Choose whether the SRMC system that will manage the Symantec Gateway Security appliance is inside [In] the network protected by Symantec Gateway Security appliance or outside [Out] the network.

   SRMC location:

   [In] Out

   By default, [In] is selected. Either press **E** to accept this default or press the right arrow (>) key to select [Out] for outside. Then press **E** to enter your selection.

   For the network in **Figure 3-3**, you would select `[Out]`. All address information you enter in the next steps is applied to the interface you select here.
3. Enter the Symantec Gateway Security appliance interface IP address. Use the arrow buttons on the front panel to enter all data. Press **E** to move to the next LCD screen when the data is complete. (For button operation instructions, see **Front panel controls on page 34**).

   IP Address:

   000.000.000.000

   This is the address of the Symantec Gateway Security appliance interface that is closest to the managing SRMC.

   For the network in **Figure 3-3**, you would enter `169.254.0.1`.

   Note: If the SRMC is offsite (as in **Figure 3-3**) or simply not behind the Symantec Gateway Security appliance in question, enter the outside interface IP address. If the SRMC is behind the Symantec Gateway Security appliance, enter the appropriate inside interface IP address.

   ---
4. Enter the netmask address for the IP address you just entered.

   Netmask:

   000.000.000.000

For the network in Figure 3-3, you would enter `255.255.255.0` as the netmask.

5 Enter the Gateway address to serve as the default gateway for the Symantec Gateway Security appliance.

If you have an internal SRMC behind an internal router, you must enter the IP address of the router interface through which the SRMC can be reached so that you can configure it from outside the internal network. If you do not have a default route, but you have an SRMC on your subnet, you can add this route later.

```
Gateway Address:

000.000.000.000
```

For the network in Figure 3-3, you would enter `169.254.0.254`.

Note: If the SRMC is behind the Symantec Gateway Security appliance and on the same subnet, you do not have to enter a Gateway Address here. You can move past this address without changing it by pressing **E**; static or default routes can be configured at a later time.

Now that Symantec Gateway Security appliance has the network configuration information it needs to locate the managing SRMC, you must enter the IP address of the SRMC host and make note of the passwords Symantec Gateway Security appliance creates for remote management.

6 Enter the SRMC host address for the SRMC host system.

```
SRMC IP Address:

000.000.000.000
```

For the network in Figure 3-3, you would enter `169.254.10.1`

Caution: Once you enter the SRMC system IP address, the Symantec Gateway Security appliance calculates and displays your remote management passwords. You MUST make note of these passwords. You can change them later, but you will need them to start the first remote management sessions between the SRMC and the Symantec Gateway Security appliance.

---

7 The SRMC password displays.

```
SRMC Password:

ltbcfetglzha
```
(for example)

Record this password in the Network configuration worksheet on page 36 and press **E** to accept it.

Later, you will enter this password into the SRMC login screen to begin a remote management session between the SRMC and the appliance. After you initially login, you can change this password through the SRMC.

Note: You cannot change your passwords on the Symantec Gateway Security appliance itself.

---

8 The SRL password displays.

```
SRL Password:
```

`xxdmmfsb` (for example)

Record this password in the Network configuration worksheet on page 36 and press **E** to accept it.

Secure Remote Login enables a user on an authorized remote system to login to the Symantec Gateway Security machine and edit Symantec Gateway Security appliance files, reboot the machine, or perform other troubleshooting or debugging tasks that are unrelated to normal Symantec Gateway Security appliance operations. All remote traffic is encrypted.

To make an SRL connection from an authorized client to the Symantec Gateway Security appliance, see Connect to Symantec Gateway Security appliance on page 54.

9 The Root password displays.

```
Root Password:
```

`h7vuvaxf` (for example)

Record this password in the Network configuration worksheet on page 36 and press **E** to accept it.

This password is used to connect directly to the Linux OS through the serial port.

You should record this password, but Symantec recommends that you do not use it to connect directly to the system. Provide this root password to customer support if your machine requires maintenance.

Note: You cannot change your passwords on the Symantec Gateway Security appliance itself.

---

10 The System ID displays.

```
System ID is

428a0d60
```
(for example)

You provide this System ID to Symantec to obtain your license key (see **Get your license key on page 45** for information on obtaining a license key). Write the System ID on the worksheet provided in this manual and press **E**.

11 You are next asked if you would like to save your setup information.

```
Save Setup?

Yes [No]
```

By default, No is selected. If you press **E** here to enter No, Symantec Gateway Security restarts the setup procedure and you must re-enter your network information.

To save your setup data, press the left (<) arrow key to select **Yes** and press **E** to save it. When you select E, the following message should display:

```
Saving Config...

Config Saved!
```

12 Press and hold down **E** to **reboot**.

The Symantec Gateway Security appliance is now ready to be configured using the SRMC. For more information see **Chapter 4, Configure using SRMC wizards**.

Display system information

Once the initial network configuration is complete, and the appliance is rebooted, the LCD enters a monitoring mode that it remains in during normal system operations. When in monitoring mode, the Symantec Gateway Security appliance alternately displays system information related to the health and status of the appliance.

It displays date, time, and status in this manner:

```
Nov 14 14:00:00
System: OK
```

The LCD next displays system version and resource utilization information:

```
V 1.0 (running)
CPU: 40% Log: 20%
```

Finally, the LCD displays the network interface load information (in packets per second):

```
In:          0/S
Out:         0/S


Aux1:        0/S
Aux2:        0/S
```

*Key:

```
In = Inside Interface = (eth0)
Out = Outside Interface = (eth1)
Aux1 = Auxiliary 1 Interface = (eth2)
Aux2 = Auxiliary 2 Interface = (eth3)
```

Use the system menu

When the Symantec Gateway Security appliance is up and running, you can access the system menu on the appliance by pressing the **E** button. The system menu contains seven options. For descriptions of the buttons on the Symantec Gateway Security appliance front panel and the functions they perform see **Front panel controls on page 34**.

The available System Menu options are:

1. Network Setup

   Use this menu option to re-enter or change network settings configured during the initial setup process. To continue to the next system menu entry, press either the down (**v**) arrow key or the right (>) arrow key.

2. Reboot

   When you press **E** on this menu item, you are prompted to select **Yes** or **No**. No is selected by default. To reboot, use an arrow button to move the cursor to Yes and press the **E** button to enter it.

3. Shutdown

   When you press **E** on this menu item, you are prompted to confirm system shutdown. Select **Yes** or **No**. Press E again to enter your selection.

4. UPS setup

   When you select this menu item, UPS (Uninterruptible Power Supply), you are prompted to choose **start** or **stop**. To use a UPS unit, select **start** and press **E**.

5. System ID

   Selecting this item causes the Symantec Gateway Security appliance to display the system's ID. You need to provide this system ID to Symantec to obtain a license key.

   Press **E** to return to the system menu once the system ID is displayed on the LCD. Press either the down arrow (**v**) key or the right arrow (>) key to move to the next menu item.

6. Factory reset

   If you press **E** on this menu item, you are prompted to confirm with **Yes** or **No**. If you select **Yes** the Symantec Gateway Security appliance resets in the following manner:

   - Network IP address information is erased.
   - SRMC workstation connection information is erased.
   - License information remains intact.

Caution: If you choose **Yes**, the appliance returns to its default state. This is the state it was in when you first received the appliance. All network information you have entered is lost as well as any configuration data. Only licensing information is retained.

7 LCD Lock

If you have enabled front panel keypad locking in system properties, selecting this item will disable the front panel controls. To unlock the LCD lock, press any button on the front panel and enter the Root password for the appliance.

Note: The front panel buttons can be locked from the SRMC. This disables the use of the buttons until the proper password is entered using the buttons. See **Use a locked keypad on page 130**.

Get your license key

You can use the Symantec Gateway Security appliance without a license key for a 30 day grace period. At any point during those 30 days, you can contact Symantec for a license key.

To get your license key and register for support, use the online license key generator from the Symantec licensing and registration site at www.symantec.com/certificate.

The Symantec Gateway Security appliance comes with the Symantec Gateway Security License Key Request and Support Registration form. This form provides a number where you can fax your license key request in the event that you cannot use the online method.

As part of the registration process, you will also be registered for one year of Gold support which includes technical support, content updates, and appliance replacements.

You must provide the Symantec Gateway Security appliance System ID and the Symantec Gateway Security product software serial number whenever requesting a license key or technical support.

- Obtain the System ID during the initial appliance setup procedure, as described in **Initial network configuration procedure on page 38**, or access it from the appliance System Menu described in **Use the system menu on page 43**.
- Locate the product serial number on the Symantec Gateway Security License Key Request and Support Registration form.

After you obtain your license key, you can enter it as part of the Symantec Gateway Security SRMC Setup Wizard procedure (see **QuickStart wizard on page 65**). If you do not enter the license key in the Setup Wizard during the initial configuration procedure, use the SRMC System Properties to enter your license key at a later time.

Restoring the Symantec Gateway Security appliance operating system

The Symantec Gateway Security CD-ROM ships with the Symantec Gateway Security appliance. It contains a Symantec Gateway Security appliance operating system restore program. In the unlikely event that a complete reinstallation of the software is required, you can boot this CD-ROM in a PC connected to the appliance.

Caution: Before you use this procedure, contact Customer Support as this operation will result in the complete overwriting of your existing Symantec Gateway Security appliance configuration. All configuration data will be lost.

The requirements for the PC running the operating system restore program are:

- A PC whose BIOS is set up to allow you to boot from a CD-ROM
- 100 MB network interface card installed
- Either a crossover cable to connect the Symantec Gateway Security appliance directly to the network interface on the PC or a connection to a switch or hub to which the appliance is attached

Note: Laptop PCs may not run the restore program properly.

During the restore process, the appliance may automatically reboot itself and perform other installation tasks. This process must be allowed to complete without interruption for a successful restore of the appliance software to its original factory condition. This process may take 15 minutes.

To restore the appliance operating system

1. Press any button on the front panel of the appliance until the System Menu displays on the LCD screen.
2. Press the down (v) arrow button until the Shutdown option appears.
3. Select the Shutdown option by pressing the E button.
4. When prompted, turn off the power using the power switch.
5. Insert the Symantec Gateway Security CD-ROM into the CD-ROM drive of your PC.
6. Reboot your PC (turn off and restart) with the Symantec Gateway Security CD in the CD drive.

7 Turn on the power to Symantec Gateway Security appliance using the power switch while pressing and holding down the Select (**S**) button on the LCD console.

8 Continue holding down the Select (**S**) button until "Select Option:" appears on the LCD display.

9 Press and release the Select (**S**) button until the "Boot From Net" option appears on the LCD display.

10 Press and release the Enter (**E**) button to begin net booting the Symantec Gateway Security appliance from the Symantec Gateway Security CD-ROM. The LCD display shows the "Loading Kernel…" message.

This step may take 15 minutes.

11 Wait until "PLEASE SWITCH OFF POWER NOW" appears on the LCD display. The restore process is now complete.

12 Turn off the Symantec Gateway Security appliance.

13 Remove the Symantec Gateway Security CD-ROM from the CD-ROM drive on your PC.

14 Restart your PC without Symantec Gateway Security CD-ROM in the PC to return it to normal service.

15 Turn on the Symantec Gateway Security appliance and perform the initial setup process again. For more information see **Initial network configuration procedure on page 38**.

The Symantec Gateway Security appliance is managed from a computer on your network using the Symantec Raptor Management Console (SRMC) Graphical User Interface.

The SRMC installs on a Windows NT or Windows 2000 machine, and can manage all Symantec Gateway Security appliance functions, including secure tunnels and hardware system management such as reboots or shutdowns. You can use the same SRMC to manage a mixture of Symantec Gateway Security appliances, VelociRaptor appliances and Symantec Enterprise Firewalls.

The SRMC provides automated wizards for:

- Symantec Gateway Security Setup
- QuickStart
- SMTP
- S2S Tunnel
- VPN Client Tunnel
- Cluster

These wizards help you get your Symantec Gateway Security appliance up and running quickly and easily. You can immediately begin securely passing traffic to and from your protected network.

Install SRMC

Install the SRMC on a system which meets the following hardware and software requirements:

- Industry Standard PC
- 233 MHz Pentium II or higher
- 128 MB RAM
- 20 MB disk space
- Ethernet card
- Windows NT 4.0 Workstation or Server with Service Pack 6a or Windows 2000 Professional or Server with Service Pack 2. Service packs can be found on the Microsoft website at http://support.microsoft.com. The system on which you install the SRMC can not be a backup or primary domain controller (PDC).
- The system must be listed on the Microsoft Windows NT 4.0 or Windows 2000 Hardware Compatibility List (HCL). Check the Microsoft web site at http://www.microsoft.com.
- TCP/IP must be installed.
- Microsoft MMC 1.2 must be installed. The executable that is used to install MC is located on the Symantec Gateway Security CD in the following location: ClientSoftware\mmc\immc.exe.
- The computer must have network connectivity with Symantec Gateway Security appliance. Ping an address on the same network as Symantec Gateway Security appliance to check.
- You must have a color monitor with a minimum resolution of 1024x768 pixels. Click the right mouse button on the background screen and select ***Properties*** from the list, then choose the ***Settings*** tab to view or modify the screen resolution.

Check your Windows NT or Windows 2000 setup before continuing:

- Your system must have Internet Explorer version 5.0 or later.
- Check the release notes and the Symantec Service and Support website (`www.symantec.com/techsupp/`) from time to time to see if new service packs are recommended.

Symantec recommends that the system and SRMC partition(s) be formatted using NTFS.

To install SRMC

1 Log on as Administrator.

2 Insert the Symantec Gateway Security appliance distribution CD-ROM.

3 Use your file browser to locate the Setup.exe file. It is located in the directory ClientSoftware\SymantecRMC\3DES (or DES).

4 Double click on the Setup.exe file.

The SRMC Setup Welcome window appears (see Figure 3-4).

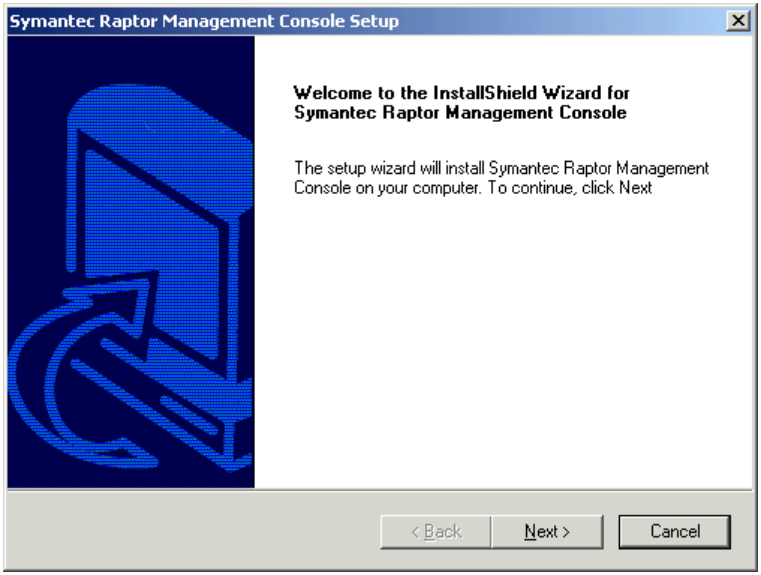

Symantec Raptor Management Console Setup
Welcome to the InstallShield Wizard for Symantec Raptor Management Console
The setup wizard will install Symantec Raptor Management Console on your computer. To continue, click Next
< Back
Next >
Cancel

Figure 3-4 The SRMC welcome window

5 Click **Next** to display the SRMC **License Agreement** window (see Figure 3-5).

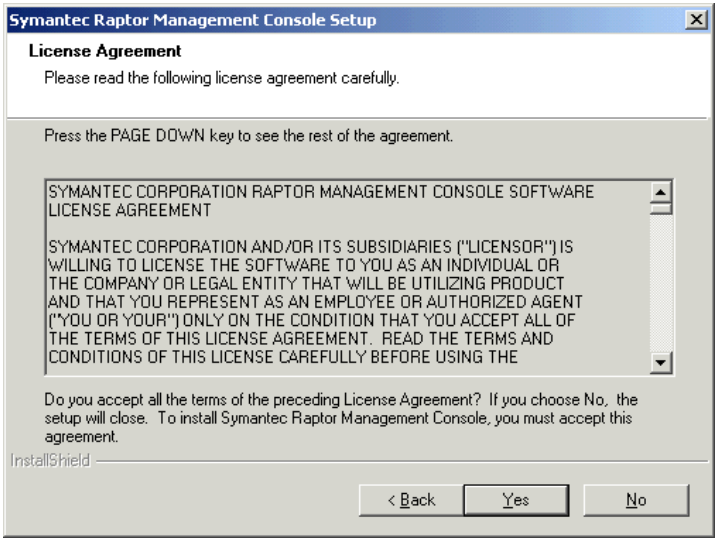

Symantec Raptor Management Console Setup
License Agreement
Please read the following license agreement carefully.
Press the PAGE DOWN key to see the rest of the agreement.
SYMANTEC CORPORATION RAPTOR MANAGEMENT CONSOLE SOFTWARE LICENSE AGREEMENT
SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("LICENSOR") IS WILLING TO LICENSE THE SOFTWARE TO YOU AS AN INDIVIDUAL OR THE COMPANY OR LEGAL ENTITY THAT WILL BE UTILIZING PRODUCT AND THAT YOU REPRESENT AS AN EMPLOYEE OR AUTHORIZED AGENT ("YOU OR YOUR") ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE CAREFULLY BEFORE USING THE
Do you accept all the terms of the preceding License Agreement? If you choose No, the setup will close. To install Symantec Raptor Management Console, you must accept this agreement.
InstallShield
< Back
Yes
No

Figure 3-5 SRMC License Agreement window

6 Read the license agreement, then click **Yes** to proceed (or **No** to exit the SMRC installation).

If you click **Yes**, the **Choose Destination Location** window is displayed (see Figure 3-6).

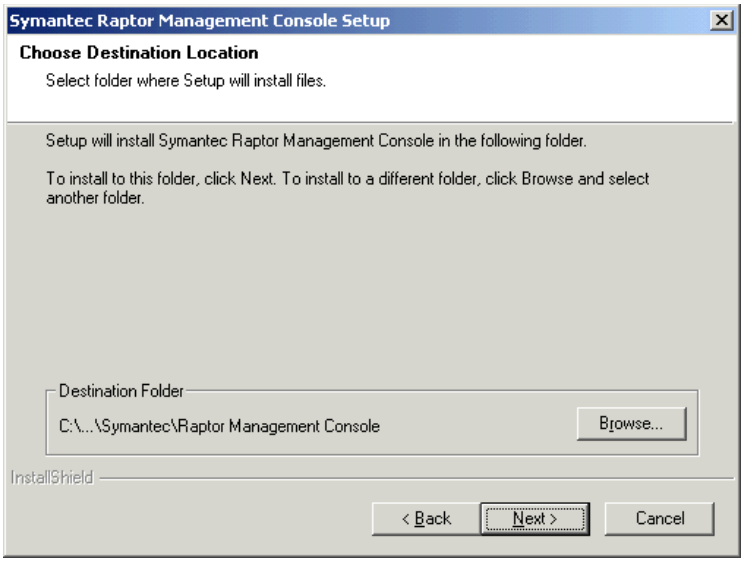

Symantec Raptor Management Console Setup
Choose Destination Location
Select folder where Setup will install files.
Setup will install Symantec Raptor Management Console in the following folder.
To install to this folder, click Next. To install to a different folder, click Browse and select another folder.
Destination Folder
C:\...\Symantec\Raptor Management Console
Browse...
InstallShield
< Back
Next >
Cancel

Figure 3-6 SRMC Choose Destination Location window

7 Click **Next** to accept the default, or specify an alternate directory path. The **Start Copying Files** window is displayed (see Figure 3-7).

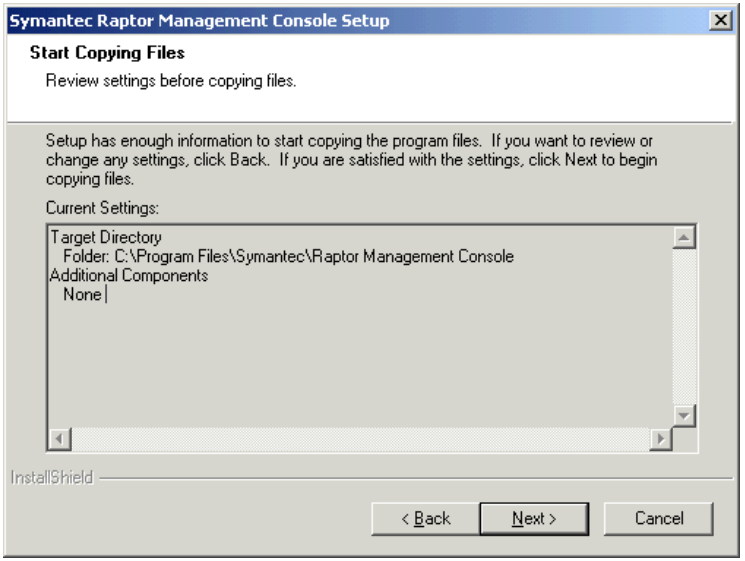

Symantec Raptor Management Console Setup
Start Copying Files
Review settings before copying files.
Setup has enough information to start copying the program files. If you want to review or change any settings, click Back. If you are satisfied with the settings, click Next to begin copying files.
Current Settings:
Target Directory
Folder: C:\Program Files\Symantec\Raptor Management Console
Additional Components
None
InstallShield
< Back
Next >
Cancel

Figure 3-7 SRMC Start Copying Files window

8 Click **Next** to install SRMC and display the **Setup Status** window (see Figure 3-8), which shows the progress of the installation.

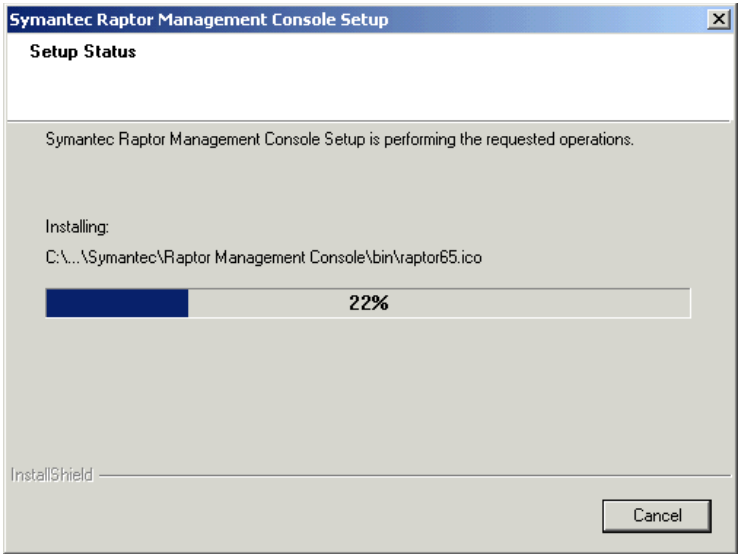


Figure 3-8 SRMC Setup Status window

When all the files are installed, SRMC InstallShield Wizard Complete window appears (see Figure 3-9).

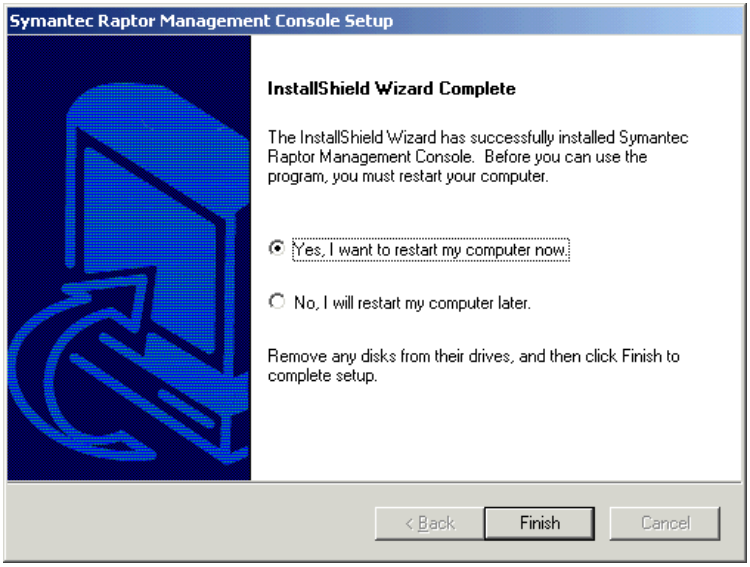

Symantec Raptor Management Console Setup
InstallShield Wizard Complete
The InstallShield Wizard has successfully installed Symantec Raptor Management Console. Before you can use the program, you must restart your computer.
Yes, I want to restart my computer now.
No, I will restart my computer later.
Remove any disks from their drives, and then click Finish to complete setup.
< Back
Finish
Cancel

Figure 3-9 SRMC InstallShield Wizard Complete window

9 Specify whether to reboot now or later, then click **Finish**.

10 When you reboot the Symantec Raptor Management Console icon and menu items are added to the desktop and programs groups. Use the Symantec Raptor Management Console icon or menu items to start SRMC.

Connect to Symantec Gateway Security appliance

After rebooting, you are ready to configure the Symantec Gateway Security appliance.

To connect to the Symantec Gateway Security appliance

1. Open SRMC by double clicking the shortcut icon placed on your desktop during installation. The Console Root window opens.
2. Expand the Symantec Enterprise Management folder.
3. Click on the **Symantec Raptor Management Console** icon in the left pane to access the **Getting Connected** taskpad (see Figure 3-10).

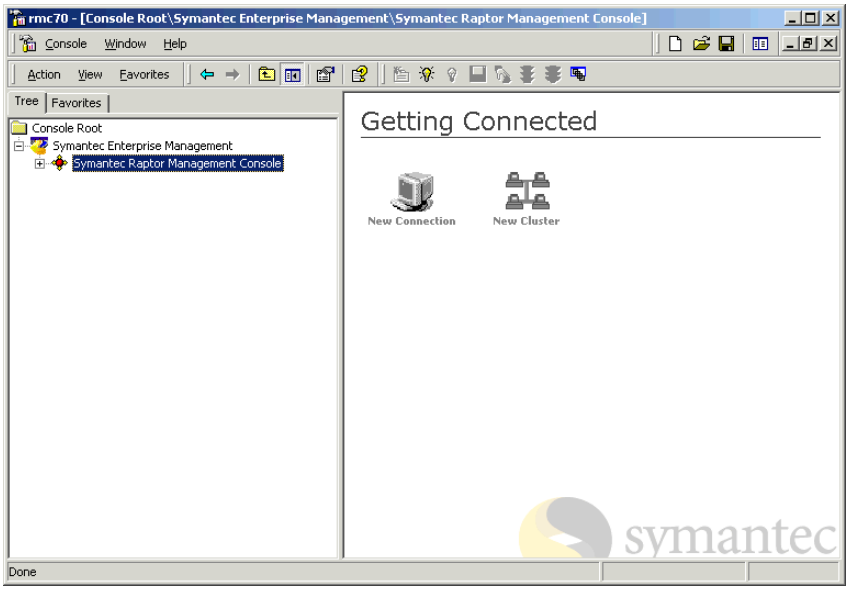


Figure 3-10 SRMC Getting Connected taskpad window

4. Click on the **New Connection** icon in the **Getting Connected** taskpad to display the SRMC logon screen (see Figure 3-11).

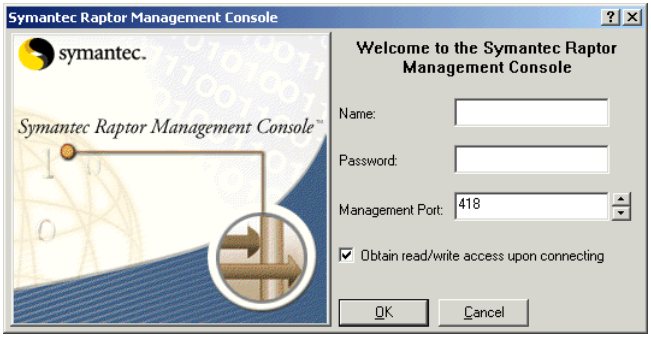


Figure 3-11 SRMC logon screen

5 Type the IP address of the Symantec Gateway Security appliance interface in the **Name** field. (The IP address you gave the appliance during initial setup.)

6 Type the **SRMC Password** that the Symantec Gateway Security appliance displayed during the initial setup procedure. (See **Initial network configuration procedure on page 38**).

7 Click **OK**.

When you attempt to connect through the SRMC for the first time, the Symantec Gateway Security appliance Setup Wizard starts automatically. It prompts you for required Symantec Gateway Security appliance configuration setup information. You must complete this wizard before you can begin managing Symantec Gateway Security appliance. See instructions in the next section.

Caution: Anyone who can access the SRMC can connect to the Symantec Gateway Security appliance once the password has been entered. Be sure to keep the password for the administering computer a secret.

Setup wizard

The Symantec Gateway Security appliance Setup wizard automatically starts when you connect to a Symantec Gateway Security appliance for the first time from the SRMC. The Setup Wizard prompts you for the following setup information that is necessary to run Symantec Gateway Security appliance:

- System name
- Domain name
- Default gateway
- License key
- System features
- Network interfaces
- Date and time

Caution: If you cancel out of this wizard without completing it at least once, you cannot connect to the Symantec Gateway Security appliance. You will have to run it again in order to access the appliance. Once you have completed the Symantec Gateway Security appliance Setup Wizard, you can use the Setup Wizard to edit system information at any time.

To configure the appliance using the Setup Wizard

1 Click on the Symantec Gateway Security Setup Wizard icon in the Configuring your Symantec System window.

The Symantec Gateway Security appliance Setup wizard automatically starts when you connect to a Symantec Gateway Security appliance for the first time from the SRMC.

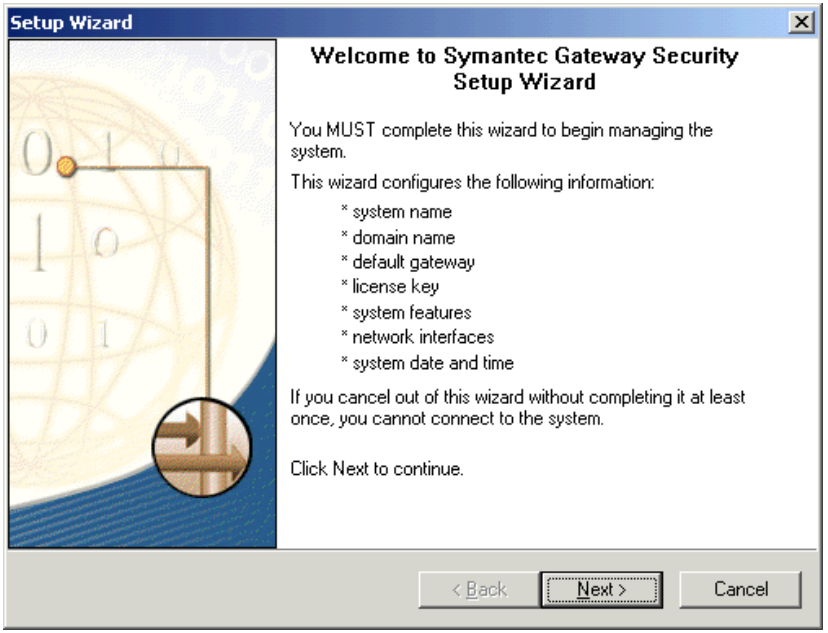

Setup Wizard
Welcome to Symantec Gateway Security Setup Wizard
You MUST complete this wizard to begin managing the system.
This wizard configures the following information:
* system name
* domain name
* default gateway
* license key
* system features
* network interfaces
* system date and time
If you cancel out of this wizard without completing it at least once, you cannot connect to the system.
Click Next to continue.
< Back
Next >
Cancel

Figure 3-12 Setup Wizard Welcome page

2 Click **Next** to began using the Setup Wizard.

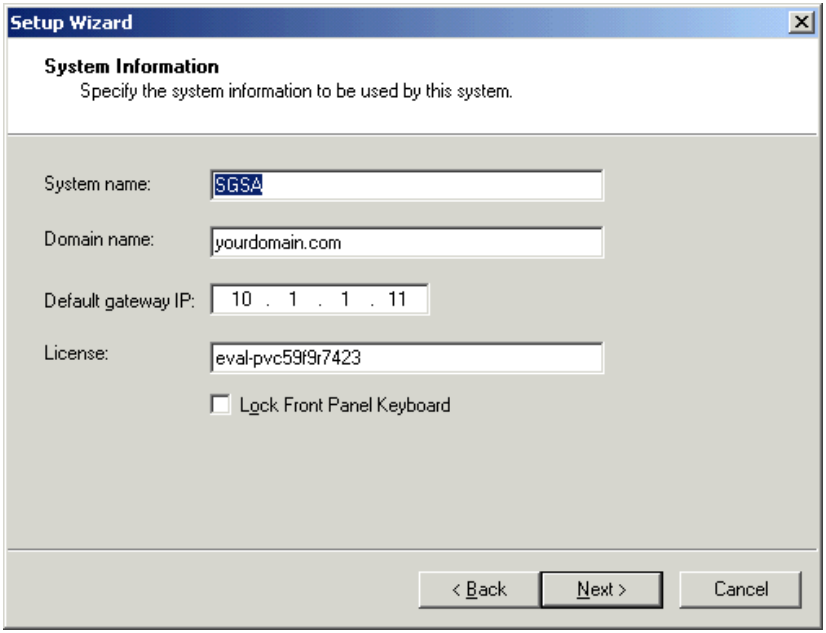


Figure 3-13 Setup Wizard System Information page

3 Enter a **System Name** for the Symantec Gateway Security appliance.

Each appliance ships with a pre-configured system name. You can change this name here if necessary.

4 Type the **Domain Name** for the system.

A domain name is displayed by default. Change this to match your domain.

5 The **Default Gateway IP** field displays the information you typed during the appliance initial setup process.

You can change this IP address, if necessary.

6 Type the **License** Key. To obtain this license key, you must provide your System ID and product serial number (see Get your license key on page 45).

If you do not type a license key here, the Symantec Gateway Security appliance will run for a 30 day grace period.

7 Check the Lock Front Panel Keyboard checkbox if you want to disable the buttons on the front panel of the appliance.

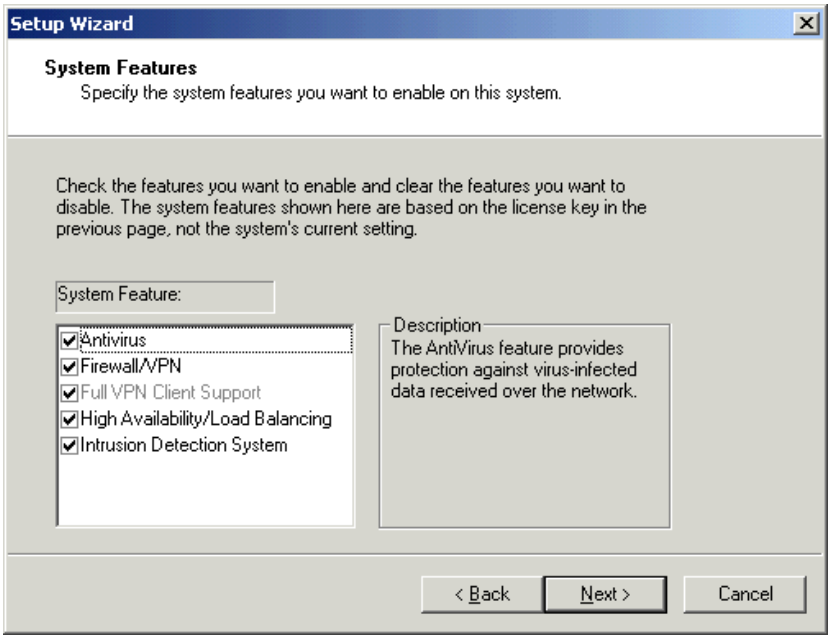

Setup Wizard
System Features
Specify the system features you want to enable on this system.
Check the features you want to enable and clear the features you want to disable. The system features shown here are based on the license key in the previous page, not the system's current setting.
System Feature:
Antivirus
Firewall/VPN
Full VPN Client Support
High Availability/Load Balancing
Intrusion Detection System
Description
The AntiVirus feature provides protection against virus-infected data received over the network.
< Back
Next >
Cancel

Figure 3-14 System Features page

8 Click **Next**.

The System Features page appears. For more information on System Features see the **Product Overview on page 7**.

9 Un-check any features you do not want to use.

You can run the Setup Wizard again to enable any feature, or use the System Features item under Base Components.

10 Click **Next**.

The **Setup Wizard Network Interfaces** page appears (see **Figure 3-15**).

You configured one ethernet interface, the interface closest to the managing SRMC system, with an IP address and netmask at the front panel during the initial appliance setup procedure. That interface should appear in the Setup Wizard Network Interfaces page.

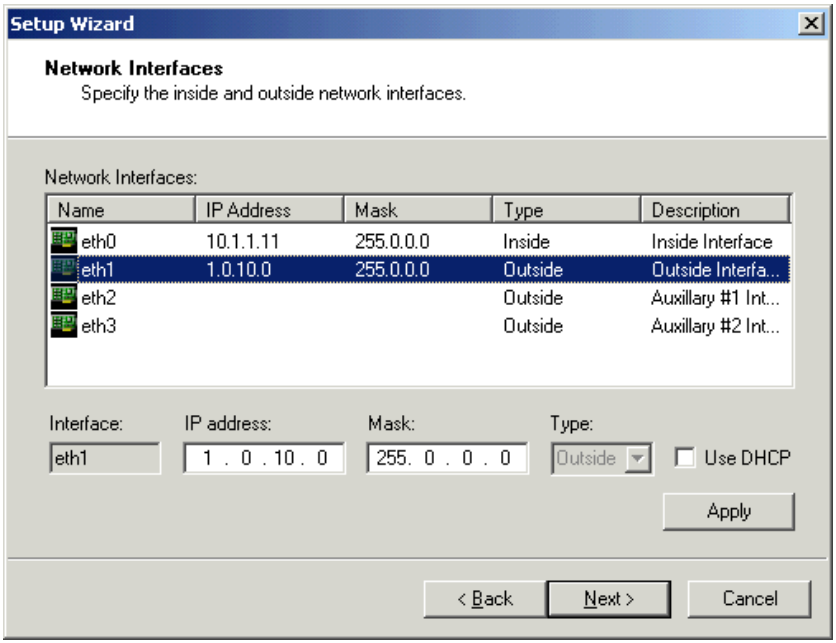


Figure 3-15 Setup Wizard Network Interfaces page

11 From the list of ethernet interfaces displayed in the **Network Interfaces** field (shown in Figure 3-15), select the interface that you want to configure.

The Symantec Gateway Security appliance provides a maximum of four ethernet connections, which are all listed. You can configure and edit the ethernet connections you see here, but you cannot add new ones.

12 After you select the interface to configure, type the interface **IP address** in the corresponding field.

13 Type the interface **netmask**.

14 From the **Type** pull-down list, select where this interface is on the network (Inside or Outside).

Note: When you configure eth0 and eth1 interfaces (Inside or Outside), the values in this field cannot be changed.

If you want to enable DHCP on the eth1 outside interface, check the **Use DHCP** check box to enable DHCP.

15 Click **Apply** to accept your edits.

16 Repeat steps 11 through 15 for each interface you are configuring. Click **Next** to move to the next page when you are finished.

17 You are then prompted to set the **Date and Time** (see Figure 3-16).

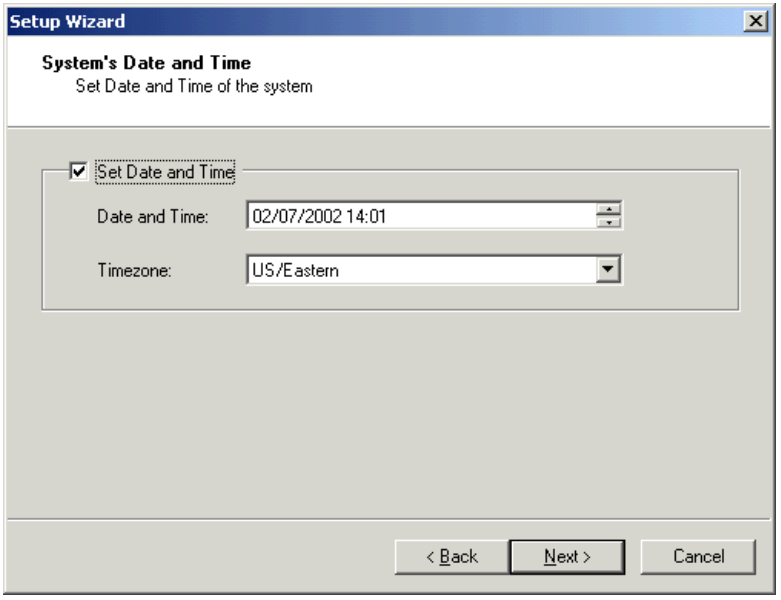


Figure 3-16 Setup Wizard System's Date and Time page

If the date and time settings are incorrect, click the **Set Date and Time** check box and edit these settings.

18 Click **Next** to complete the setup wizard.

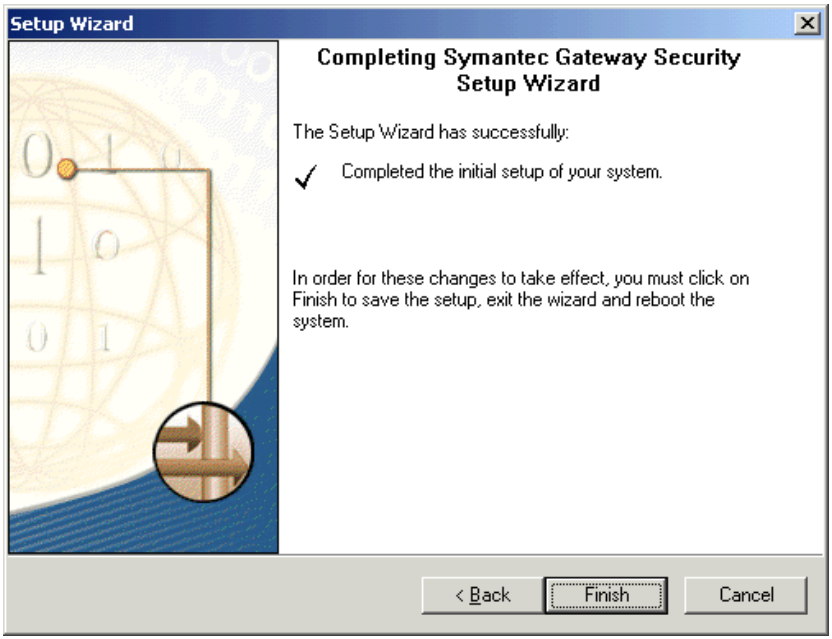

Setup Wizard
Completing Symantec Gateway Security Setup Wizard
The Setup Wizard has successfully:
Completed the initial setup of your system.
In order for these changes to take effect, you must click on Finish to save the setup, exit the wizard and reboot the system.
< Back
Finish
Cancel

Figure 3-17 Setup Wizard completion page

19 Click **Finish**.

After you have successfully completed the Symantec Gateway Security appliance Setup Wizard (see **Figure 3-17**), you are prompted to reboot the appliance. When the reboot is complete, the Symantec Gateway Security appliance is up and running.

Note: You must access the logon screen again to connect to the Symantec Gateway Security appliance (see **Connect to Symantec Gateway Security appliance on page 54**).

Once you have completed the Symantec Gateway Security appliance Setup Wizard the first time, you can access it again from the Configuring your Symantec System taskpad and edit any system information. (See **Figure 4-1**).

Chapter 4

Firewall

The SRMC provides two automated wizards for setting up the firewall features of the Symantec Gateway Security appliance:

- The QuickStart Wizard provides a quick way to configure mail, FTP, and web services for the Firewall.
- The SMTP Wizard provides a quick way to configure rules to provide anti-spamming and anti-relay protection and prevent your internal mail server from being used as a spam relay.

For setting up firewall configurations beyond those detailed in this chapter, refer to the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide,* provided on the Symantec Gateway Security CD-ROM as a PDF file.

QuickStart wizard

Use the QuickStart wizard to quickly set up your mail, FTP, and web services on the firewall of the Symantec Gateway Security appliance.

After you connect to the Symantec Gateway Security appliance, the configuration taskpad appears in the right pane. Click on the QuickStart icon (see **Figure 4-1**) to access the QuickStart wizard. You can re-run the wizard to make changes at any time by selecting the Symantec Gateway Security appliance system icon in the left pane. If you have taskpads turned on, the configuration taskpad containing the QuickStart wizard icon will appear in the right pane.

The QuickStart wizard gives you two firewall configuration options:

- Configure mail services.

  The Symantec Gateway Security appliance's secure Simple Mail Transfer Protocol (SMTP) proxy, (SMTPD) enables you to pass SMTP mail by application proxy. SMTPD supports transparent addressing, allowing authorized internal systems to contact external systems directly. It also checks all traffic entering and leaving your domain for known sendmail attacks, and it uses heuristics to detect and record new types of attacks. The QuickStart wizard can prepare all these configurations for you.

  Note: You can use the SMTP Wizard to set up your mail server with anti-spamming parameters without configuring Web access as well. (See **SMTP Wizard on page 70**).

- Configure the appliance to allow inside users to access web and FTP services.

  At this point, your inside machines are cut off from the Internet. Allowing HTTP and FTP access involves creating two simple rules called interface-based rules. They allow web and file transfer protocol access for your inside users. The QuickStart wizard creates these rules for you.

To use the Quickstart wizard for Symantec Gateway Security appliance firewall setup

1. In the left pane, select the icon of the Symantec Gateway Security appliance for which you are configuring mail and/or web access to display the **Configuring your Symantec System** taskpad (see **Figure 4-1**).

   If the taskpad is not displayed, pull down the **View** menu and choose **Taskpad**.

   You can re-enter the wizard to make changes at any time, by selecting the system icon to display the Configuring your Symantec System Taskpad.

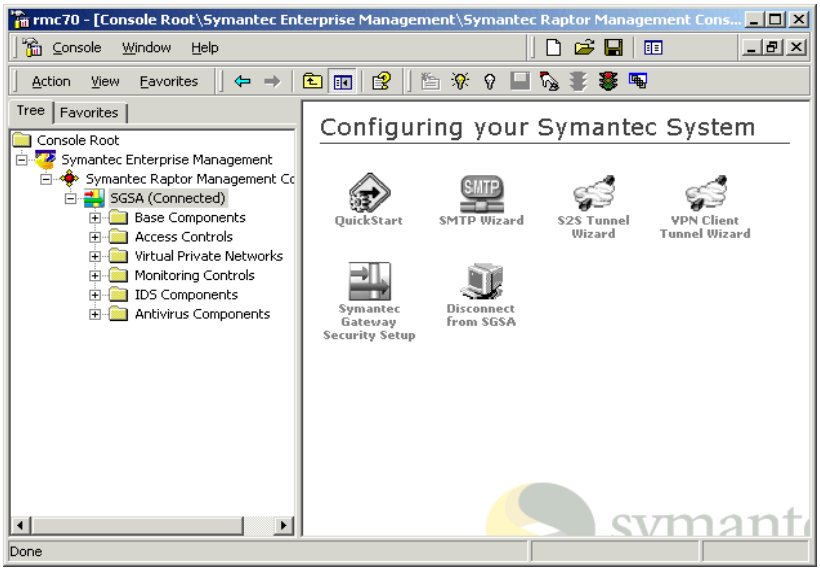


Figure 4-1 Configuring your Symantec System taskpad

2 Click the **QuickStart** icon in the taskpad. The **Welcome to the QuickStart Wizard** screen appears (see Figure 4-2).

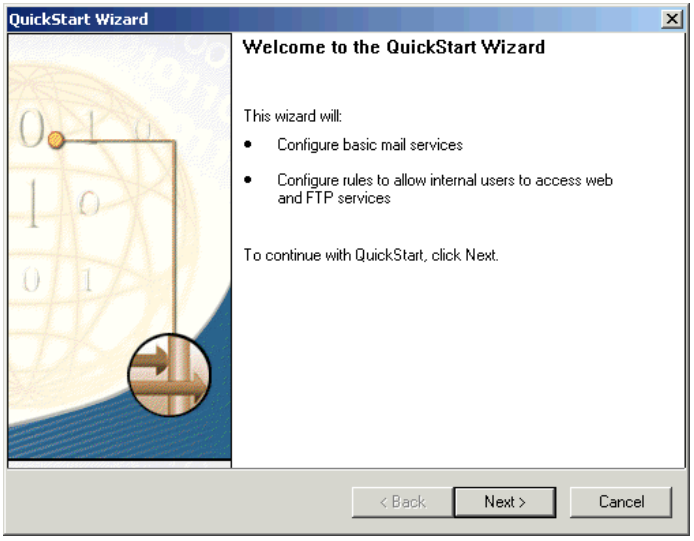

QuickStart Wizard
Welcome to the QuickStart Wizard
This wizard will:
Configure basic mail services
Configure rules to allow internal users to access web and FTP services
To continue with QuickStart, click Next.
< Back
Next >
Cancel

Figure 4-2 QuickStart Wizard introduction

3 Click **Next** to begin using the QuickStart wizard.

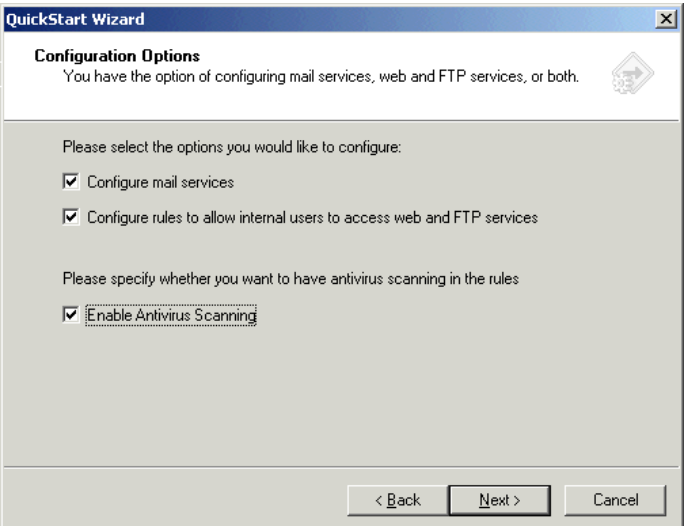

QuickStart Wizard
Configuration Options
You have the option of configuring mail services, web and FTP services, or both.
Please select the options you would like to configure:
Configure mail services
Configure rules to allow internal users to access web and FTP services
Please specify whether you want to have antivirus scanning in the rules
Enable Antivirus Scanning
< Back
Next >
Cancel

Figure 4-3 QuickStart Wizard Configuration Options

4 The Configuration Options screen provides three check boxes: one to configure mail services, one to configure web and FTP services, and one to enable antivirus scanning in the rules for mail services and/or web and FTP services.

- If you check **Configure mail services**, when you **click Next** (with or without checking **Enable Antivirus Scanning**), the following screen prompts you for the IP address of your mail server. Continue at step 5.
- If you check **Configure rules to allow internal users to access web and FTP services** and/or **Enable Antivirus Scanning**, QuickStart automatically configures these services without requiring any further input. If these are the only options you select, continue at step 10.

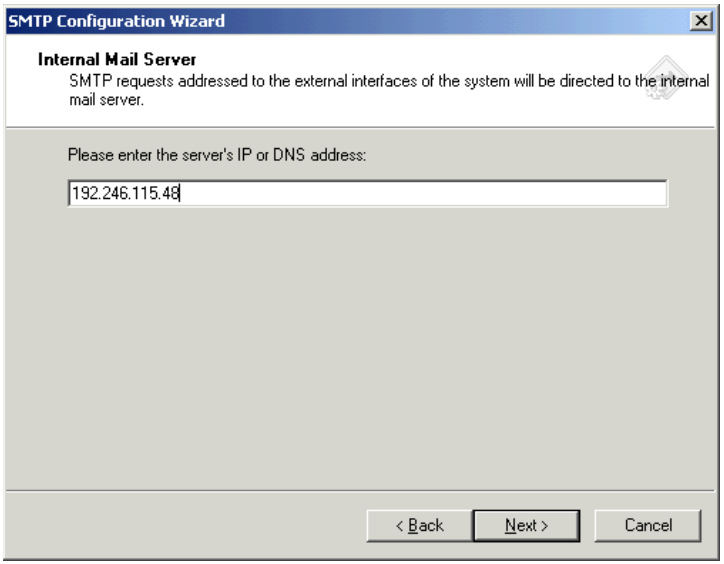

SMTP Configuration Wizard
Internal Mail Server
SMTP requests addressed to the external interfaces of the system will be directed to the internal mail server.
Please enter the server's IP or DNS address:
192.246.115.48
< Back
Next >
Cancel

Figure 4-4 Internal Mail Server screen

5 On the Internal Mail Server screen, enter the IP address or DNS name of your site's internal mail server.

In specifying an internal mail server, you are indicating where SMTP mail addressed to the appliance's external interface will be directed.

6 Click **Next** to display the **Allow Internal Hosts Out** screen (see Figure 4-5).

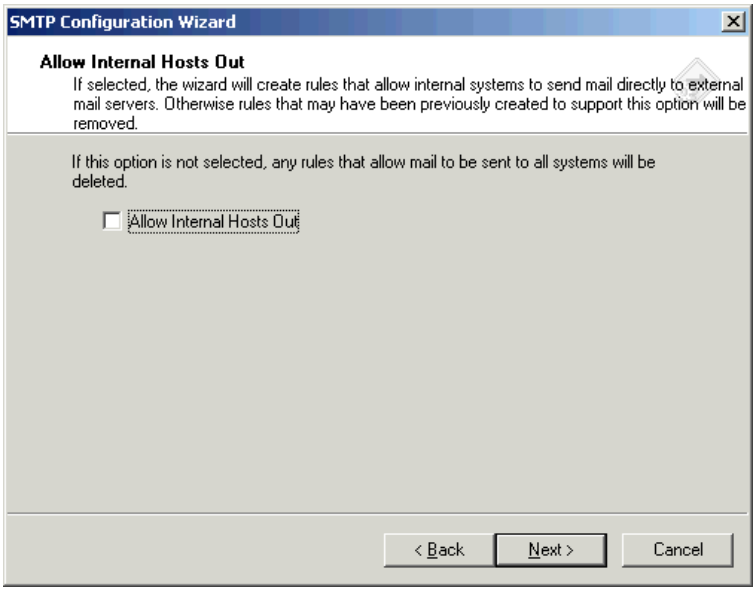

SMTP Configuration Wizard
Allow Internal Hosts Out
If selected, the wizard will create rules that allow internal systems to send mail directly to external mail servers. Otherwise rules that may have been previously created to support this option will be removed.
If this option is not selected, any rules that allow mail to be sent to all systems will be deleted.
Allow Internal Hosts Out
< Back
Next >
Cancel

Figure 4-5 Allow Internal Hosts Out

7 To allow all internal hosts to send mail directly to all external systems, check the **Allow Internal Hosts Out** check box.

This allows internal systems to bypass the internal mail server.

8 Click **Next**.

The QuickStart wizard prepares the configurations you have specified.

9 Click **Next** when the progress bar shows that the preparations are complete.

10 The final Quickstart wizard screen displays, allowing you to choose when you want to save and reconfigure the Symantec Gateway Security appliance.

11 Make your selection and click **Finish**. If you choose not to reconfigure now, make sure that you do so at a later point.

Quickstart firewall configuration results

When you have finished configuring your mail server and/or web and FTP services, the QuickStart wizard automatically creates the necessary rules and redirected services to provide mail and/or web service to your network.

When QuickStart sets up your mail server, depending upon your wizard selections, it configures the following:

- A rule to allow all systems to send mail to the internal mail server
- A rule to allow the internal mail server to send mail to all systems
- A rule to allow hosts on the inside network to send mail to all systems (only if the **Allow Internal Hosts Out** check box is selected)
- A service redirection to redirect **SMTP** traffic arriving at the appliance's outside interface to the mail server
- Antivirus scanning of mail traffic (only if the **Enable Antivirus Scanning** check box is selected)

In specifying an Internal mail server, you are indicating where SMTP mail addressed to the Symantec Gateway Security appliance's external interface is directed.

When QuickStart configures access to web and FTP services, it also configures a rule from the inside interface to the Universe, allowing all internal systems to access HTTP and FTP services destined for anywhere. Antivirus scanning of HTTP and FTP traffic is performed if the **Enable Antivirus Scanning** check box is selected.

Note: For setting up firewall configurations beyond those detailed in the QuickStart wizard, refer to the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide,* provided on the Symantec Gateway Security CD-ROM as a PDF file.

SMTP Wizard

The SMTP Wizard provides a quick way to configure rules to provide anti-spamming and anti-relay protection and prevent your internal mail server from being used as a spam relay.

Because SRMC automatically creates the necessary rules for SMTP service when you use the wizard to configure your mail server, you can set up anti-spamming parameters on one particular rule created by the wizard. The rule that allows “all systems to send mail to the internal mail server” should contain your anti-spam restrictions.

To run the SMTP Wizard

1 In the left pane, click on the icon of the appliance on which you want to perform the configuration.

The Configuring your Symantec System taskpad appears in the right pane.

If the taskpad is not visible, pull down the **View** menu and click **Taskpad**.

2 In the right pane, start the wizard by clicking the SMTP Wizard icon.

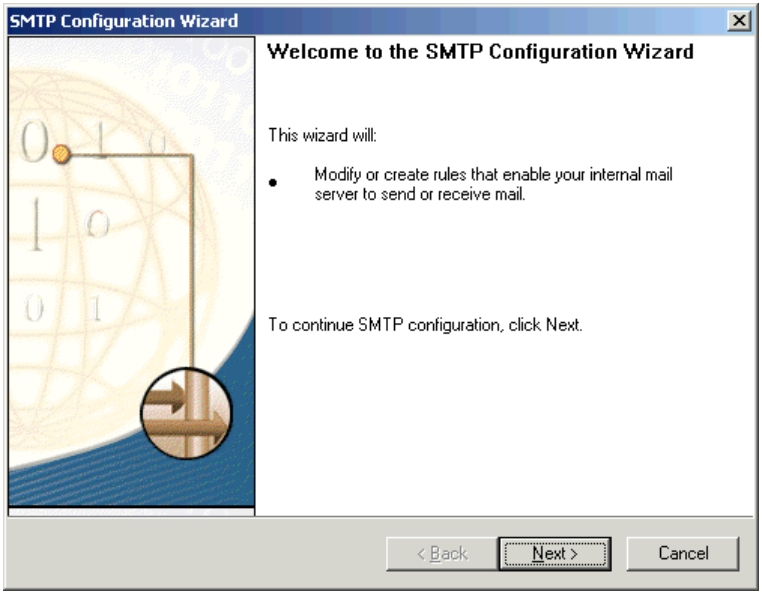

SMTP Configuration Wizard
Welcome to the SMTP Configuration Wizard
This wizard will:
Modify or create rules that enable your internal mail server to send or receive mail.
To continue SMTP configuration, click Next.
< Back
Next >
Cancel

Figure 4-6 SMTP Configuration Wizard Welcome screen

3 Click **Next**.

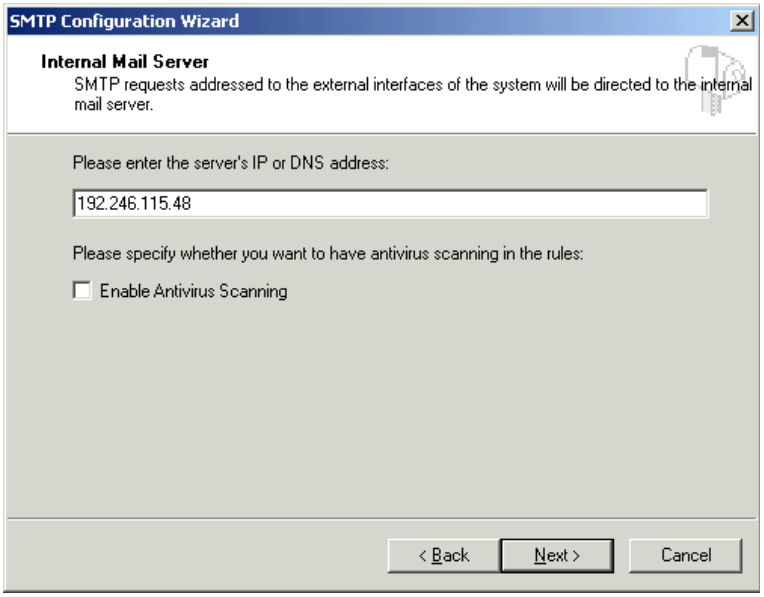

SMTP Configuration Wizard
Internal Mail Server
SMTP requests addressed to the external interfaces of the system will be directed to the internal mail server.
Please enter the server's IP or DNS address:
192.246.115.48
Please specify whether you want to have antivirus scanning in the rules:
Enable Antivirus Scanning
< Back
Next >
Cancel

Figure 4-7 Internal Mail Server

4 Enter the IP address or DNS name of your internal mail server.

5 If you want antivirus scanning to be performed on SMTP traffic, check the **Enable Antivirus Scanning** check box.

6 Click **Next**.

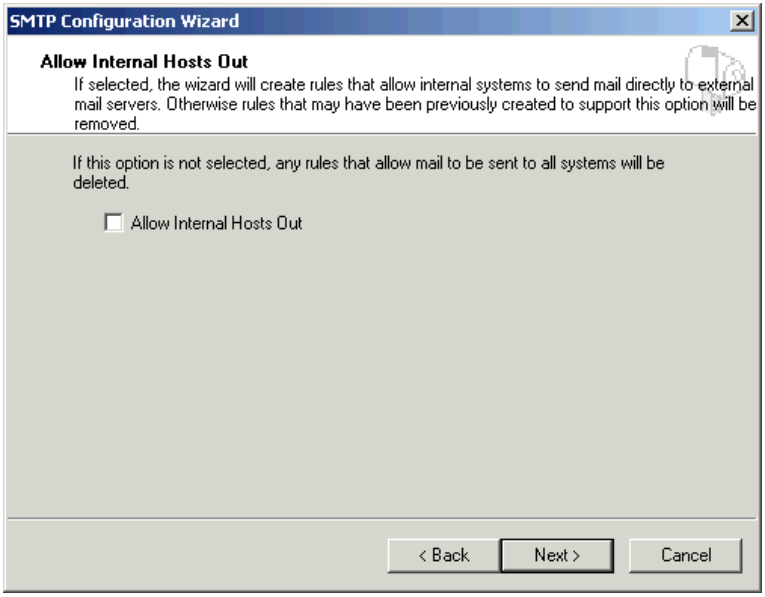

SMTP Configuration Wizard
Allow Internal Hosts Out
If selected, the wizard will create rules that allow internal systems to send mail directly to external mail servers. Otherwise rules that may have been previously created to support this option will be removed.
If this option is not selected, any rules that allow mail to be sent to all systems will be deleted.
Allow Internal Hosts Out
< Back
Next >
Cancel

Figure 4-8 Allow Internal Hosts Out screen

7 If you want to create a rules that will allow the internal systems to send mail directly to external mail servers, check the **Allow Internal Hosts Out** check box.

8 Click **Next**.

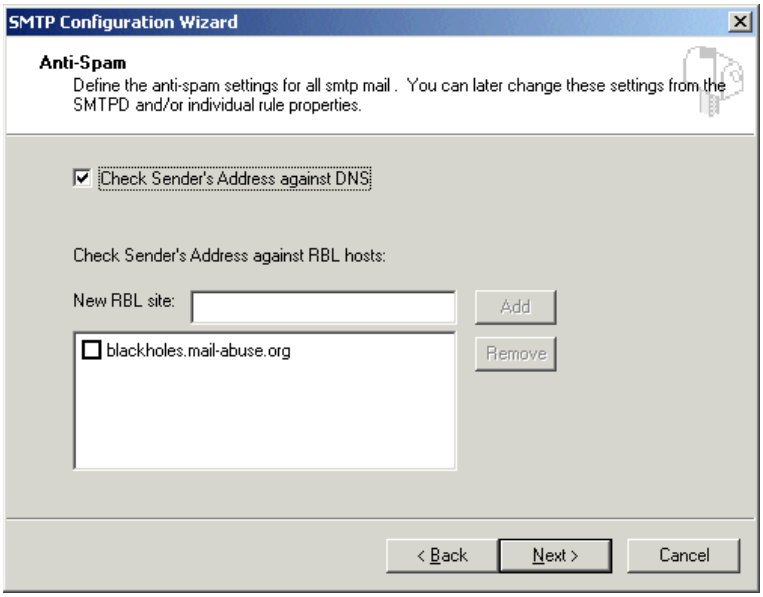

SMTP Configuration Wizard
Anti-Spam
Define the anti-spam settings for all smtp mail . You can later change these settings from the SMTPD and/or individual rule properties.
Check Sender's Address against DNS
Check Sender's Address against RBL hosts:
New RBL site:
Add
blackholes.mail-abuse.org
Remove
< Back
Next >
Cancel

Figure 4-9 Anti-Spam screen

9 On the Anti-Spam page, define the anti-spam settings for all SMTP mail.

The **Check Sender's Address against DNS** check box is checked by default. This validates the originator's envelope address by checking the format and ensuring the domain name is fully qualified. It also checks whether an MX record exists for the domain name in DNS (Domain Name System). E-mail from recipients who fail the DNS-registration test is rejected.

Check Sender's address against RBL hosts checks the sender's address against the addresses in the a list of known spam originators known as the Realtime Blackhole List (RBL). Any incoming connection attempts will be denied if the address is found in the RBL.

If you check the list provided, the RBL of the Mail Abuse Prevention System project is used. You can also enter the domain name of another RBL provider in **New RBL Site** field and add it to the list of RBL sites by clicking **Add**.

10 Click **Next**.

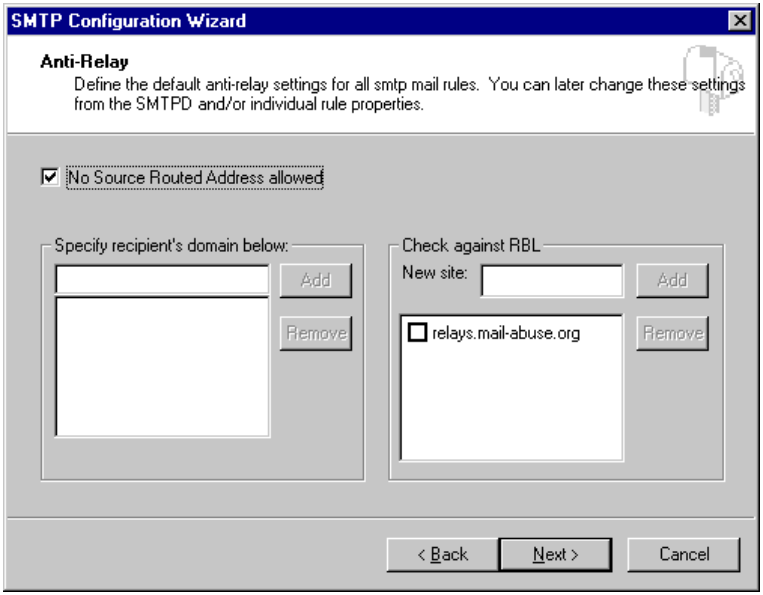


Figure 4-10 Anti-Relay screen

11 On the Anti-Relay page, define the default anti-relay settings for your SMTP mail rules.

No Source Routed Address allowed is enabled by default. This causes SMTP to refuse all e-mail to addresses specified using source-routing syntax, such as @host1,@host2:user@symantec.com.

If you disable this check box and specify a Domain name in the **Specify recipient's domain name** field, the SMTP proxy will only accept the e-mail if the final destination is one of the acceptable recipient domains.

If you disable this check box and do not specify a recipient domain, the SMTP proxy will accept e-mail for all addresses, source-routed or not.

You can also specify an RBL site against which the address should be checked.

12 Click **Next**.

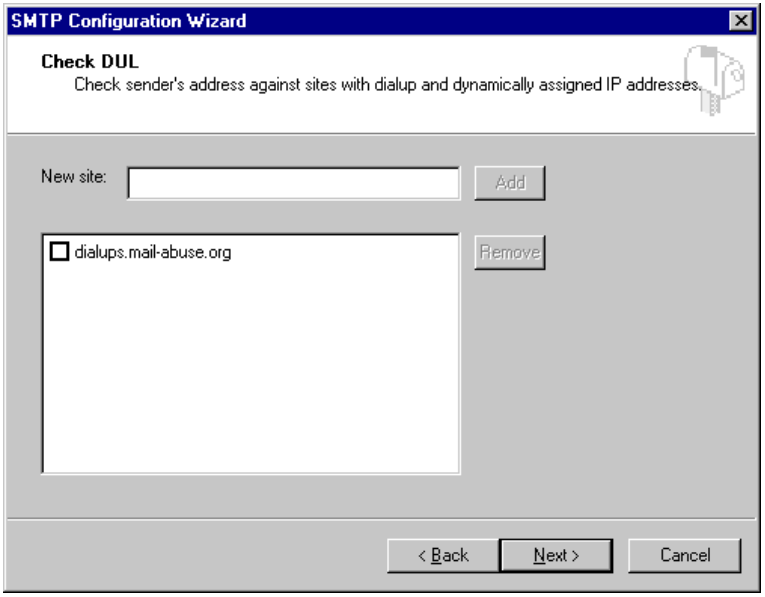


Figure 4-11 Check DUL screen

13 On the Check DUL page, specify the domain name of a dial-up user list (DUL), or check the domain name provided.

As with the RBL, this instructs SMTP to check the sender's address against a list of sites with dialup and dynamically assigned IP addresses of mass e-mailers who spam using direct connections to their victims' mail servers without using their ISP's mail server as a relay or gateway.

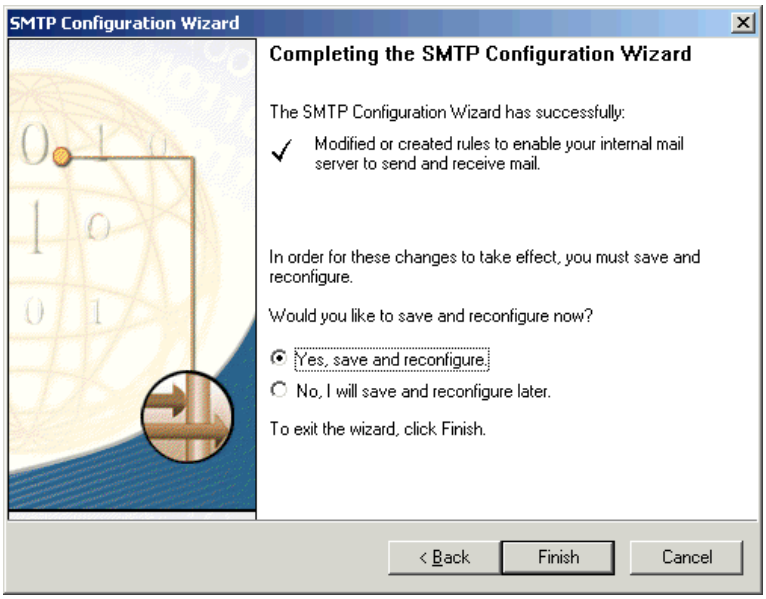

SMTP Configuration Wizard
Completing the SMTP Configuration Wizard
The SMTP Configuration Wizard has successfully:
Modified or created rules to enable your internal mail server to send and receive mail.
In order for these changes to take effect, you must save and reconfigure.
Would you like to save and reconfigure now?
Yes, save and reconfigure.
No, I will save and reconfigure later.
To exit the wizard, click Finish.
< Back
Finish
Cancel

Figure 4-12 Completing the SMTP Configuration Wizard

14 Select the appropriate radio button to indicate whether you will save and reconfigure the appliance now or later, then click **Finish** to complete the wizard.

Note: You can later change the anti-spam and anti-relay settings from the SMTPD Proxy Properties page and/or the individual rule properties. For more information, see the *Symantec Enterprise Firewall and Symantec VPN Configuration Guide*.

Chapter 5

VPN

This chapter describes the use of the two tunnel wizards, S2S (site to site) and the VPN Client. You can use these wizards to connect to remote hosts or clients. If you would prefer not to use these wizards, refer to the procedures for configuring secure tunnels in the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide,* provided in PDF format.

Note: In order to use VPN Client tunnels, you will need the full VPN function crossgrade license.

SRMC provides two tunnel wizards:

- **S2S Tunnel Wizard**: Use this wizard to configure site to site (LAN to LAN) secure tunnels.
- **VPN Client Tunnel Wizard**: Use this wizard to configure tunnels to VPN clients.

Note: Before you use the tunnel wizards, you may want to configure the network entity and security gateway building blocks that you will select for your tunnel, although the wizards do let you create these. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for Network Entity, Security Gateway, and Certificate configuration procedures.

To access either of the tunnel wizards in SRMC

1. Select the system icon for the Symantec Gateway Security appliance you are managing. The **Configuring your Symantec System** taskpad appears (see Figure 4-1).
2. Click on the **S2S Tunnel Wizard** icon or the **VPN Client Tunnel Wizard** icon to begin configuring your tunnel.

Note: The Symantec Gateway Security appliance can create VPN tunnels to other Symantec Gateway Security appliances, VelociRaptor appliances, systems running Symantec Enterprise Firewall with VPN, or to any IPsec compliant device. It can also create tunnels to remote clients running Symantec Enterprise VPN clients with the full VPN function crossgrade license.

Configure S2S tunnels using the wizard

The secure tunnel configuration displayed in Figure 5-1 is an example of a site to site tunnel. The following pages walk you through the process of using the S2S Tunnel Wizard to set up the components of this tunnel.

In Figure 5-1, there are two sites. Each site is protected by a Symantec Gateway Security appliance. West is the local appliance in this example and East is the remote VPN server. The goal of this configuration is to establish a VPN tunnel uniting the subnets behind each firewall.

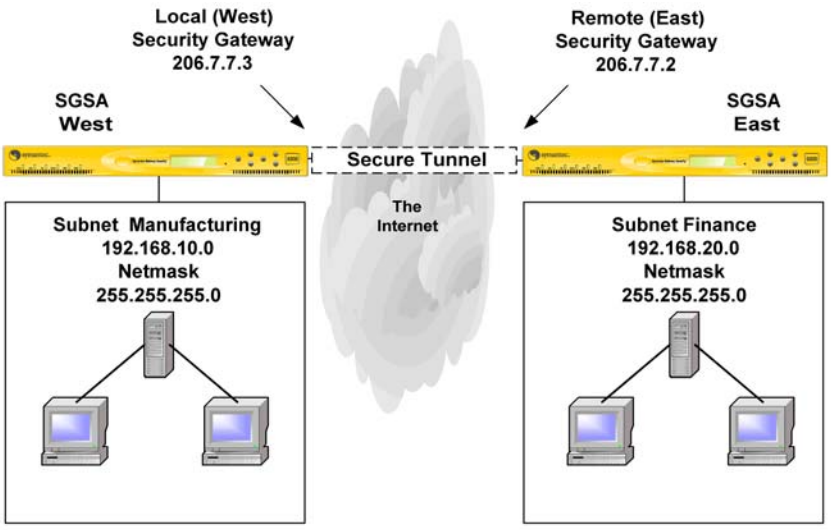


Figure 5-1 Site to site secure tunnel

To begin using the wizard, from the SRMC **Configuring your Symantec System** taskpad (see Figure 4-1), click the **S2S Tunnel Wizard** icon. The Introduction screen shown in Figure 5-2 appears.

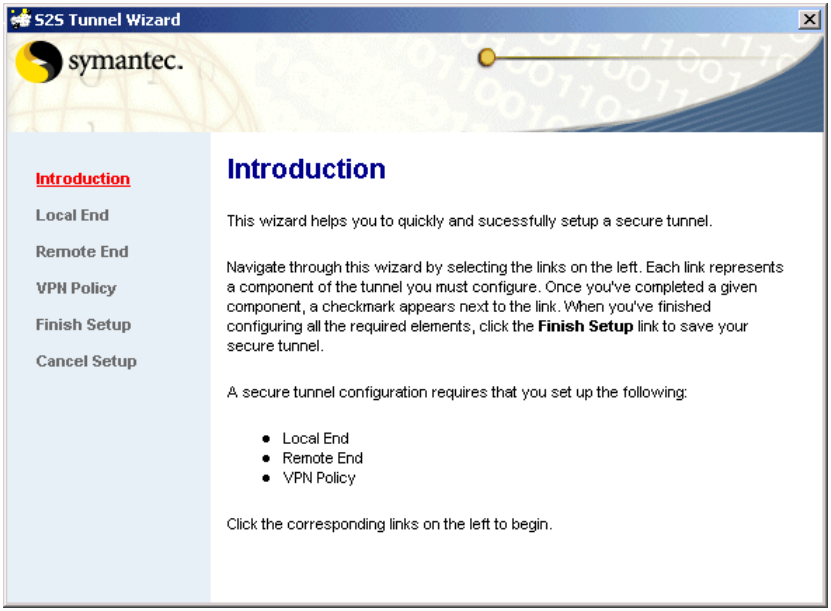

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Introduction
This wizard helps you to quickly and sucessfully setup a secure tunnel.
Navigate through this wizard by selecting the links on the left. Each link represents a component of the tunnel you must configure. Once you've completed a given component, a checkmark appears next to the link. When you've finished configuring all the required elements, click the Finish Setup link to save your secure tunnel.
A secure tunnel configuration requires that you set up the following:
Local End
Remote End
VPN Policy
Click the corresponding links on the left to begin.

Figure 5-2 Introduction screen: S2S Tunnel Wizard

As the Introduction screen explains (see Figure 5-2), click on the links on the left side of the screen to configure the corresponding component of the tunnel. It is suggested that you follow the links in the order they appear, starting with **Local End**.

In the various wizards screens, you are asked to select a combination of security gateways, network entities, and users with which to build your tunnel. If you have not configured these tunnel components before beginning the wizard, you can create a new security gateway, network entity, or user from within the wizard.

To configure the Local End of a S2S tunnel using the S2S tunnel wizard

1 From the wizard Introduction page, click on the **Local End** link on the left side of the screen.

The **Local End** configuration page appears (see Figure 5-3).

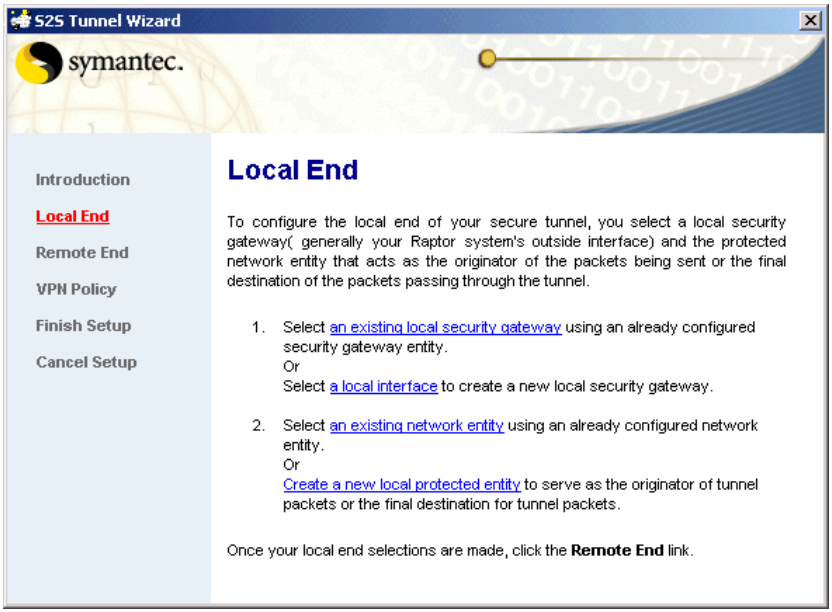

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Local End
To configure the local end of your secure tunnel, you select a local security gateway(generally your Raptor system's outside interface) and the protected network entity that acts as the originator of the packets being sent or the final destination of the packets passing through the tunnel.
1. Select an existing local security gateway using an already configured security gateway entity.
Or
Select a local interface to create a new local security gateway.
2. Select an existing network entity using an already configured network entity.
Or
Create a new local protected entity to serve as the originator of tunnel packets or the final destination for tunnel packets.
Once your local end selections are made, click the Remote End link.

Figure 5-3 Local End: S2S Tunnel Wizard

2 Step 1 on the Local End screen gives you two ways to select the local security gateway:

- By selecting an existing security gateway
- By using a local interface to create a new security gateway

For the network example in Figure 5-1, we will create the local security gateway using the local interface.

Click the **local interface** link available in step 1 on the configuration page to display the pull-down menu (see Figure 5-4).

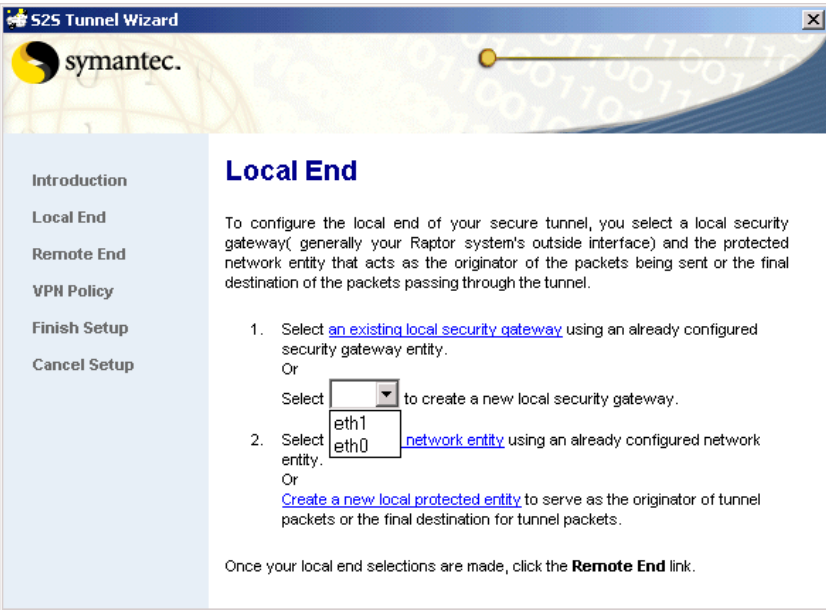

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Local End
To configure the local end of your secure tunnel, you select a local security gateway(generally your Raptor system's outside interface) and the protected network entity that acts as the originator of the packets being sent or the final destination of the packets passing through the tunnel.
1. Select an existing local security gateway using an already configured security gateway entity.
Or
Select
to create a new local security gateway.
eth1
eth0
2. Select
network entity using an already configured network entity.
Or
Create a new local protected entity to serve as the originator of tunnel packets or the final destination for tunnel packets.
Once your local end selections are made, click the Remote End link.

Figure 5-4 Local interface pull-down menu

3 From the interfaces available in the pull-down menu, select the outside interface, **eth0**, to become your local security gateway. This displays the **New Security Gateway** dialog box.

4 In the dialog box, type a name for your gateway. Our example uses *West* (see Figure 5-5).

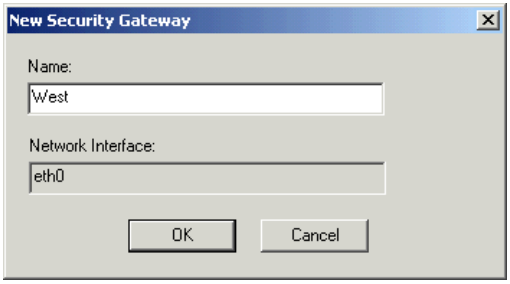


Figure 5-5 New Security Gateway dialog box: local end

5 Click **OK**; your new security gateway will be used as the local security gateway.

6 Step 2 of the Local End screen gives you two ways to specify the originator or the endpoint for tunnel packets:

- By selecting an existing network entity
- By creating a new local protected entity

In this case, we will create a new entity to represent our manufacturing subnet shown in Figure 5-1.

From the second part of step 2, select the **Create a new local protected entity** link to display a pull-down menu of allowed entity types (see Figure 5-6).

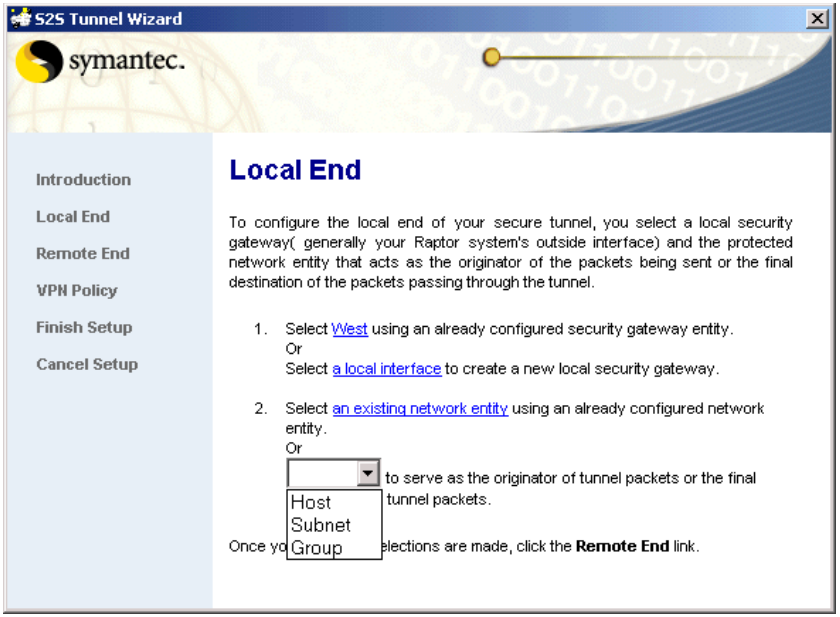

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Local End
To configure the local end of your secure tunnel, you select a local security gateway(generally your Raptor system's outside interface) and the protected network entity that acts as the originator of the packets being sent or the final destination of the packets passing through the tunnel.
1. Select West using an already configured security gateway entity.
Or
Select a local interface to create a new local security gateway.
2. Select an existing network entity using an already configured network entity.
Or
to serve as the originator of tunnel packets or the final tunnel packets.
Host
Subnet
Group
Once yo elections are made, click the Remote End link.

Figure 5-6 Local protected entity pull-down menu

7 In this example, we select **Subnet** from the pull-down menu to create the 192.168.10.0 manufacturing subnet displayed in Figure 5-1. A New Subnet dialog box appears (see Figure 5-7).

Figure 5-7 New Subnet dialog: local end

8 In the dialog box, type a **Name** for your subnet entity, in this case, *manufacturing*, and type the IP address of the subnet, in this case 192.168.10.0.

9 Click **OK**; your subnet entity will be used as the local network entity.

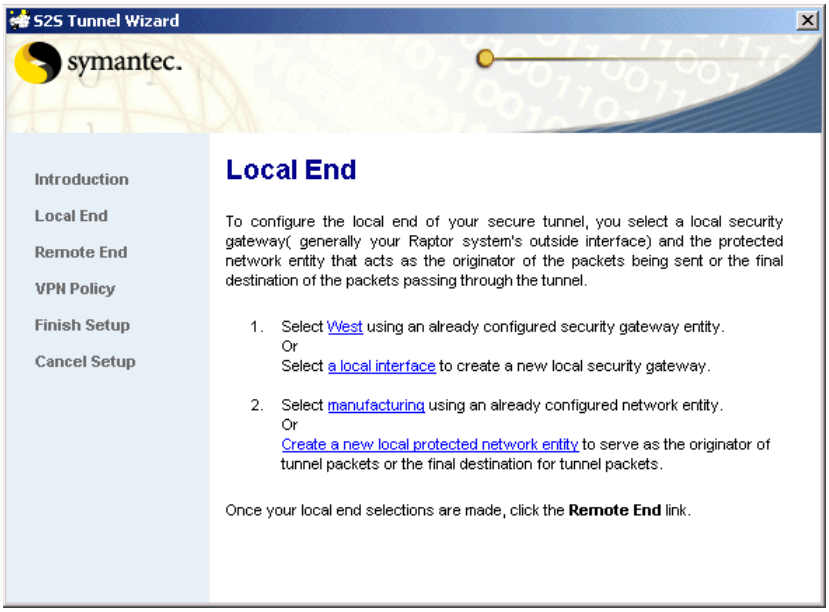

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Local End
To configure the local end of your secure tunnel, you select a local security gateway(generally your Raptor system's outside interface) and the protected network entity that acts as the originator of the packets being sent or the final destination of the packets passing through the tunnel.
1. Select West using an already configured security gateway entity.
Or
Select a local interface to create a new local security gateway.
2. Select manufacturing using an already configured network entity.
Or
Create a new local protected network entity to serve as the originator of tunnel packets or the final destination for tunnel packets.
Once your local end selections are made, click the Remote End link.

Figure 5-8 Completed Local End screen: S2S Tunnel Wizard

The local end of your secure tunnel is now configured.

To configure the Remote End of an S2S tunnel using the S2S Tunnel Wizard

1 Click the Remote End link on the left side of the screen.

The Remote End screen is displayed with a check mark beside the Local End link to indicate completion, as shown in **Figure 5-9**.

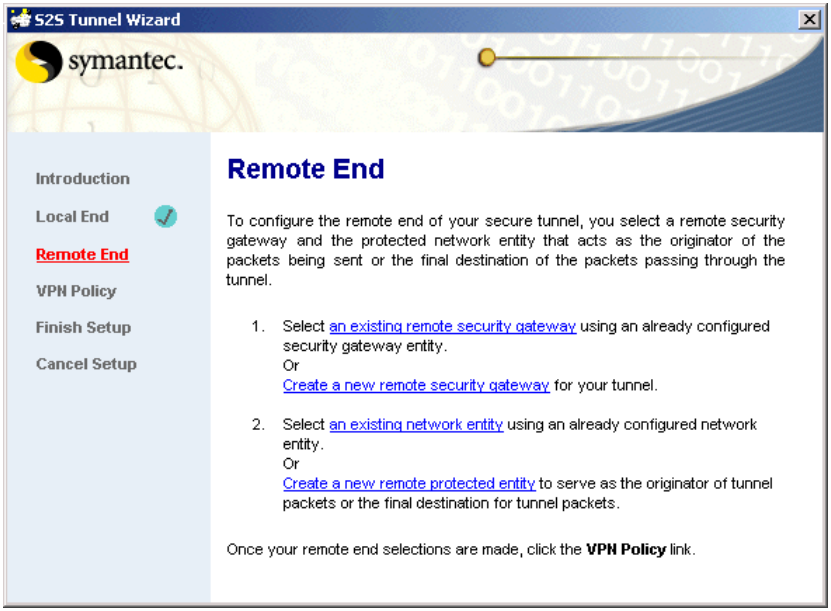

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Remote End
To configure the remote end of your secure tunnel, you select a remote security gateway and the protected network entity that acts as the originator of the packets being sent or the final destination of the packets passing through the tunnel.
1. Select an existing remote security gateway using an already configured security gateway entity.
Or
Create a new remote security gateway for your tunnel.
2. Select an existing network entity using an already configured network entity.
Or
Create a new remote protected entity to serve as the originator of tunnel packets or the final destination for tunnel packets.
Once your remote end selections are made, click the VPN Policy link.

Figure 5-9 Remote End Screen: S2S Tunnel Wizard

2 Step 1 on the Remote End screen gives you two ways to select the remote security gateway:

- By selecting an existing remote security gateway entity
- By creating a new remote security gateway entity

For the network example in Figure 5-1, we will create a new remote security gateway for the appliance called East by selecting the **Create a new remote security gateway** link available in step 1. The **New Security Gateway** dialog box appears (see Figure 5-10).

New Security Gateway
Name:
East
Enter the IP address or a DNS resolvable name for your new Security Gateway.
206.7.7.2
Authentication method
Certificate
Shared Key:
Note that both gateways of a tunnel must be using the same authentication method (and the same shared secret if using it).
OK
Cancel

Figure 5-10 New Security Gateway dialog box: Remote End

3 In the dialog box, type a **Name** and an **IP address** for your remote gateway. In this case, *East* and 206.7.7.2. Also, decide which authentication method is to be used (see **Figure 5-10**). In this example, we have selected Certificate for authentication.

For details on authentication, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

4 Click **OK**; the name of your new security gateway will be used as the Remote Security Gateway.

5 Step 2 of the Remote End screen gives you two ways to specify the remote originator or endpoint for tunnel packets:

- By selecting an existing network entity
- By creating a new protected network entity

In this case, we will create a new entity to represent the remote finance subnet displayed in **Figure 5-1**.

From the second part of step 2, select the **Create a new remote protected entity** link. A pull-down menu appears (see **Figure 5-11**).

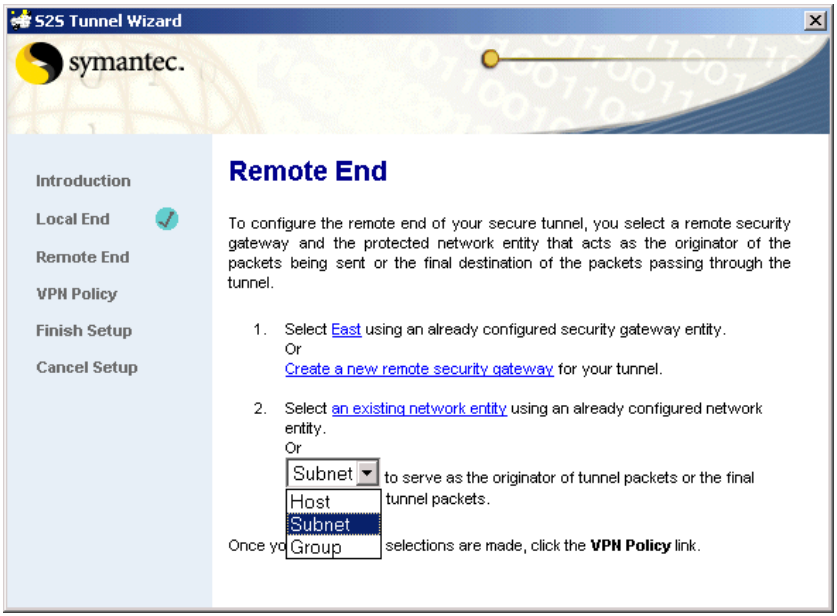

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Remote End
To configure the remote end of your secure tunnel, you select a remote security gateway and the protected network entity that acts as the originator of the packets being sent or the final destination of the packets passing through the tunnel.
1. Select East using an already configured security gateway entity.
Or
Create a new remote security gateway for your tunnel.
2. Select an existing network entity using an already configured network entity.
Or
Subnet to serve as the originator of tunnel packets or the final tunnel packets.
Host
Subnet
Group
Once yo selections are made, click the VPN Policy link.

Figure 5-11 Remote protected entity pull-down menu

6 Select **Subnet** from the pull-down menu to create the 206.7.7.2 finance subnet displayed in Figure 5-1. The **New Subnet** dialog box appears (see Figure 5-12).

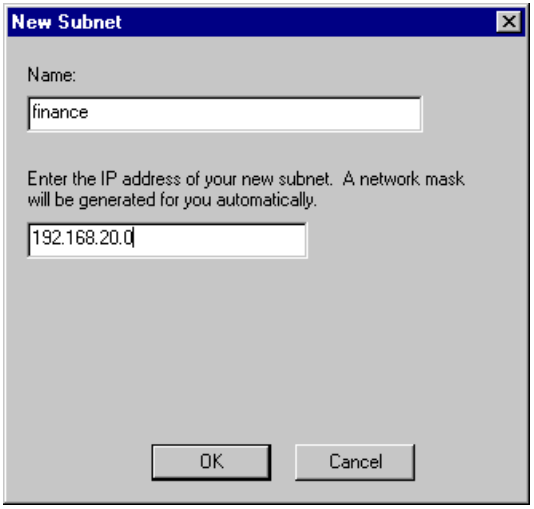


Figure 5-12 New Subnet dialog box: Remote End

7 In the dialog box, type a **Name** for your subnet entity and the IP address of the subnet, in this case *finance* and 192.168.20.0.

8 Click **OK**; your new subnet entity will be used as the remote network entity.

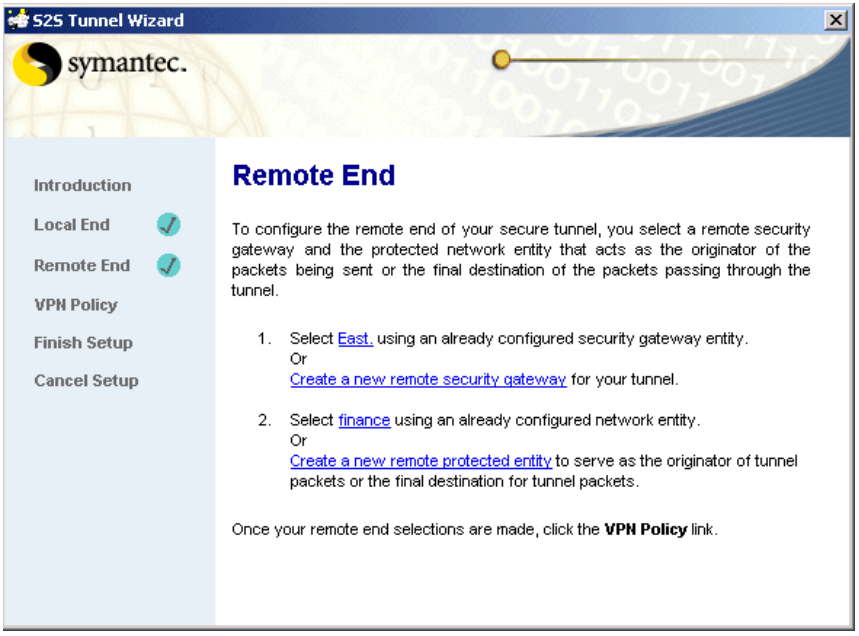

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Remote End
To configure the remote end of your secure tunnel, you select a remote security gateway and the protected network entity that acts as the originator of the packets being sent or the final destination of the packets passing through the tunnel.
1. Select East. using an already configured security gateway entity.
Or
Create a new remote security gateway for your tunnel.
2. Select finance using an already configured network entity.
Or
Create a new remote protected entity to serve as the originator of tunnel packets or the final destination for tunnel packets.
Once your remote end selections are made, click the VPN Policy link.

Figure 5-13 Completed Remote End screen: S2S Tunnel Wizard

The remote end of your secure tunnel is now configured.

To configure the VPN Policy of a S2S Tunnel

1 Click on the VPN Policy link on the left side of the screen to display the **VPN Policy** configuration page.

A check mark appears beside the Remote End link to indicate completion (see Figure 5-14.)

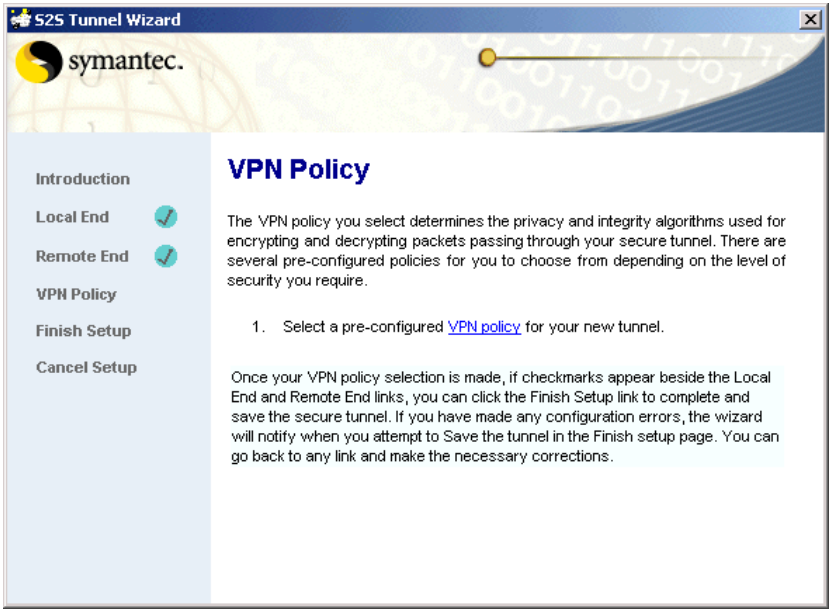

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
VPN Policy
The VPN policy you select determines the privacy and integrity algorithms used for encrypting and decrypting packets passing through your secure tunnel. There are several pre-configured policies for you to choose from depending on the level of security you require.
1. Select a pre-configured VPN policy for your new tunnel.
Once your VPN policy selection is made, if checkmarks appear beside the Local End and Remote End links, you can click the Finish Setup link to complete and save the secure tunnel. If you have made any configuration errors, the wizard will notify when you attempt to Save the tunnel in the Finish setup page. You can go back to any link and make the necessary corrections.

Figure 5-14 VPN Policy screen: S2S Tunnel Wizard

The Symantec Gateway Security appliance ships with several pre-configured VPN policies.

2 From step 1 in this VPN Policy screen (see Figure 5-14), click the **VPN policy** link.

The VPN policy pull-down menu appears (see Figure 5-15).

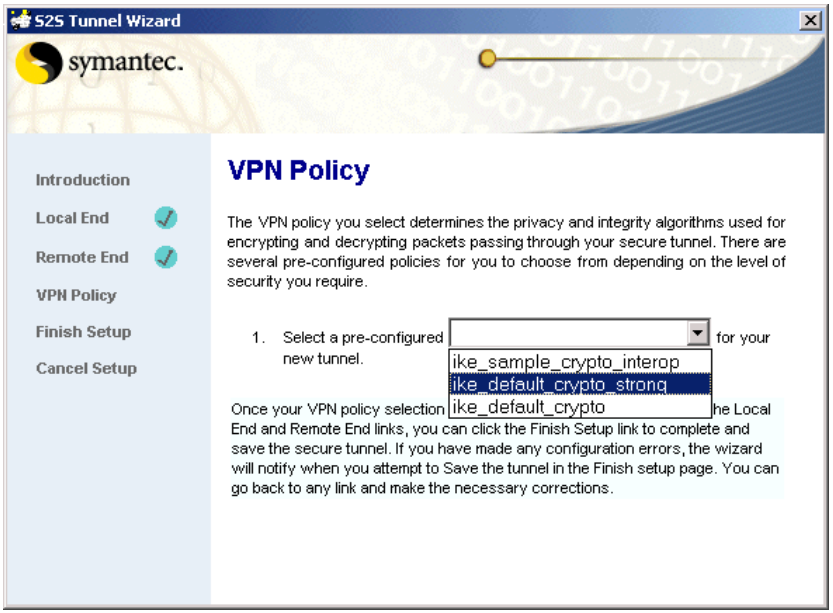

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
VPN Policy
The VPN policy you select determines the privacy and integrity algorithms used for encrypting and decrypting packets passing through your secure tunnel. There are several pre-configured policies for you to choose from depending on the level of security you require.
1. Select a pre-configured for your new tunnel.
ike_sample_crypto_interop
ike_default_crypto_strong
ike_default_crypto
Once your VPN policy selection he Local End and Remote End links, you can click the Finish Setup link to complete and save the secure tunnel. If you have made any configuration errors, the wizard will notify when you attempt to Save the tunnel in the Finish setup page. You can go back to any link and make the necessary corrections.

Figure 5-15 VPN policy pull-down menu

3 Select an existing policy from the pull-down menu.

In this case, we are selecting the pre-configured *ike_default_crypto_strong* policy. Once your tunnel is configured, you can exit the wizard and access the property page for this VPN policy to view its components.

Caution: The VPN policy must be the same for both ends of the tunnel. Administrators must exchange this information. Refer to the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for details.

To finish the configuration of the S2S tunnel

1 Click the **Finish Setup** link on the left side.

The Finish Setup screen is displayed, with a check mark beside the VPN Policy link to indicate that the VPN Policy configuration is complete.

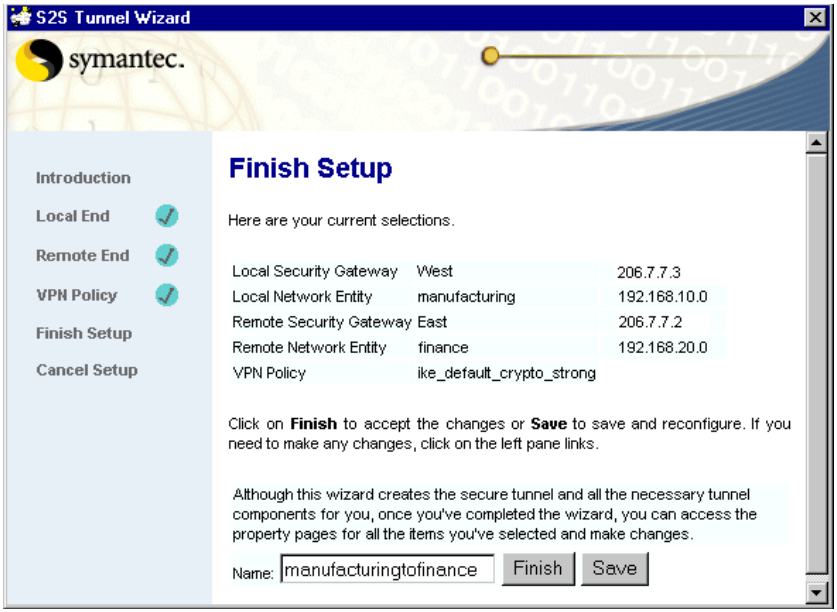

S2S Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Finish Setup
Here are your current selections.
Local Security Gateway West 206.7.7.3
Local Network Entity manufacturing 192.168.10.0
Remote Security Gateway East 206.7.7.2
Remote Network Entity finance 192.168.20.0
VPN Policy ike_default_crypto_strong
Click on Finish to accept the changes or Save to save and reconfigure. If you need to make any changes, click on the left pane links.
Although this wizard creates the secure tunnel and all the necessary tunnel components for you, once you've completed the wizard, you can access the property pages for all the items you've selected and make changes.
Name: manufacturingtofinance
Finish
Save

Figure 5-16 Finish Setup: S2S Tunnel Wizard

The Finish Setup screen (see Figure 5-16) displays the selections you have made in the previous screens. If you have failed to make a required selection, that item appears with the word "undefined" beside it in the Finish Setup screen and that link has no check mark beside it on the left side of the screen.

If you were unable to complete any of the screens up to this point, simply click on that screen's link in the left pane to go back.

2 The Finish Setup screen assigns a default name to your tunnel.

In the **Name** field, enter your own name for the secure tunnel before you save.

In Figure 5-16, we have named the tunnel *manufacturingtofinance.*

3 If each left pane item has a check mark beside it, you can now click the **Save** button to save your secure tunnel configuration.

If there are any errors in your configuration, a message notifies you that the configuration is invalid. You can then click on any of the left side links to make the necessary corrections.

When you have completed and exited the tunnel wizard, you can view your configuration in SRMC by expanding the Virtual Private Networks folder,

clicking on the Secure Tunnels, and then double clicking the entry for the tunnel you created (see Figure 5-17).

You can also open the property pages for the entities and the tunnel you have just created. From those property pages, you can check your configuration and make any edits, if necessary. Refer to the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for more detailed tunnel configuration information.

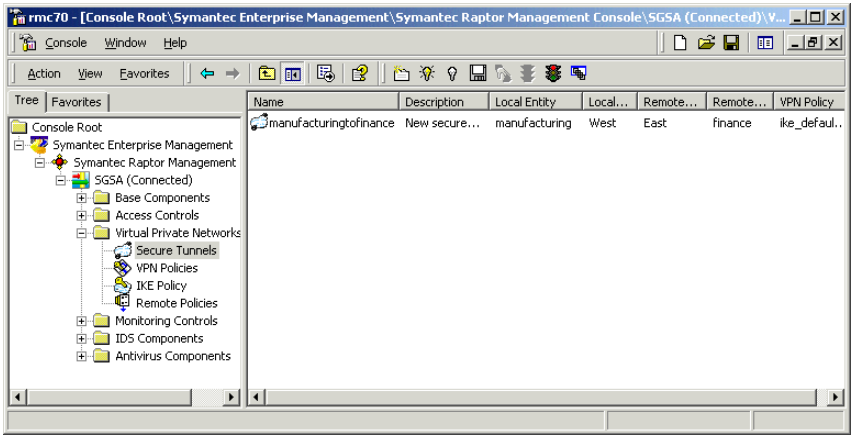


Figure 5-17 Configured S2S secure tunnel in SRMC

You must configure both ends of the tunnel. Run the S2S Wizard on the remote end of the tunnel, and specify the setup information in the reverse manner as the procedure in Configure S2S tunnels using the wizard on page 79. For example, local would be *East* and *finance* and remote would be *West* and *manufacturing*.

Configure VPN Client tunnels using the wizard

The VPN client tunnel configuration displayed in Figure 5-18 is an example of a secure tunnel set up between a LAN behind a Symantec Gateway Security appliance and a VPN client in the field. The following pages walk you through the process of using the VPN Client Tunnel Wizard to set up the components of this tunnel.

In Figure 5-18, West is once again our local VPN Server in this example and JSmith is the user name for our Symantec Enterprise VPN Client (SEVPN). The goal of this configuration is to establish a VPN uniting the subnet behind the local Symantec Gateway Security appliance with the SEVPN client JSmith.

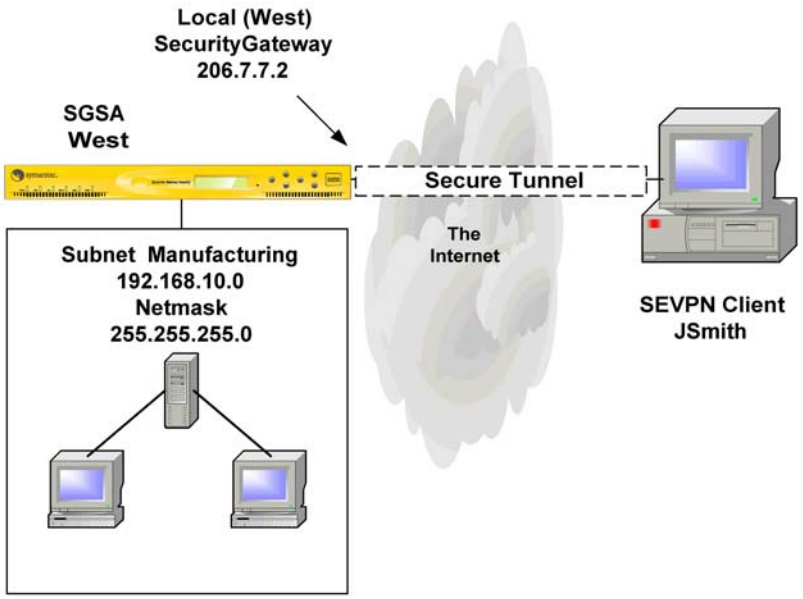


Figure 5-18 VPN Client secure tunnel

To configure a VPN Client tunnel

To begin using the wizard, from the SRMC **Configuring your Symantec System** taskpad (see Figure 4-1), click the **VPN Client Tunnel Wizard** icon. The Introduction screen shown in Figure 5-2 appears.

The wizard screens as well as the configuration procedures for both the S2S and VPN Client Tunnel Wizards in our examples are identical with one exception, configuring the remote end. Because the local end in this second example is the same as in the first example, only the differing remote end VPN Client configuration procedure is detailed in the following pages. For more information see Configure S2S tunnels using the wizard on page 79.

To configure the Remote End of the VPN Client Tunnel

1 Click on the **Remote End** link on the left side of the screen. The Remote End configuration page appears (see Figure 5-19).

The Remote End screen of the VPN Client Tunnel Wizard gives you three ways to specify the single entity that will serve as both the remote security gateway and the tunnel endpoint.

- By selecting an existing IKE-enabled user
- By creating a new IKE-enabled user
- By selecting an existing user group

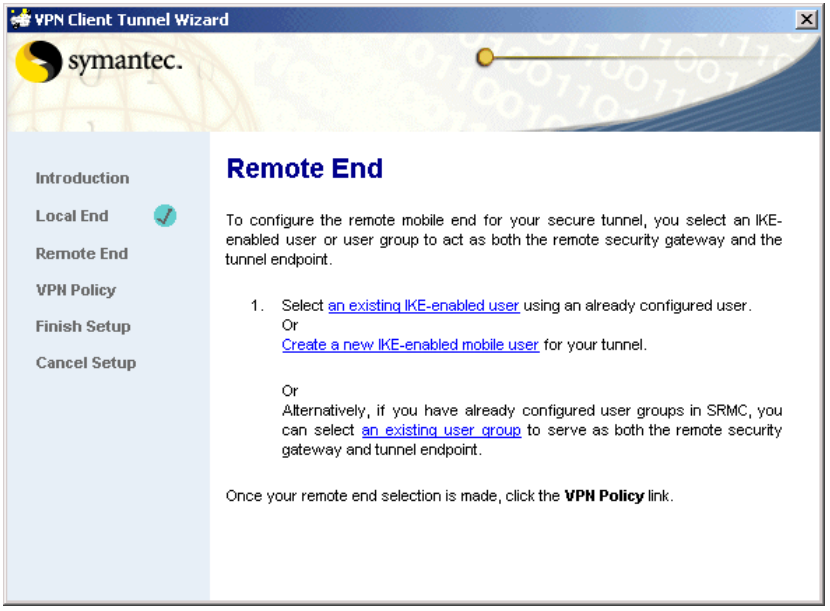

VPN Client Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Remote End
To configure the remote mobile end for your secure tunnel, you select an IKE-enabled user or user group to act as both the remote security gateway and the tunnel endpoint.
1. Select an existing IKE-enabled user using an already configured user.
Or
Create a new IKE-enabled mobile user for your tunnel.
Or
Alternatively, if you have already configured user groups in SRMC, you can select an existing user group to serve as both the remote security gateway and tunnel endpoint.
Once your remote end selection is made, click the VPN Policy link.

Figure 5-19 Remote End screen: VPN Client Tunnel Wizard

For the network example in Figure 5-18, we are creating a new VPN Client user named Jsmith.

2 From the Remote End VPN Client Wizard page (see Figure 5-19), click the **Create a new IKE-enabled VPN Client user** link available in step 1. The New IKE-enabled User dialog box appears (see Figure 5-20).

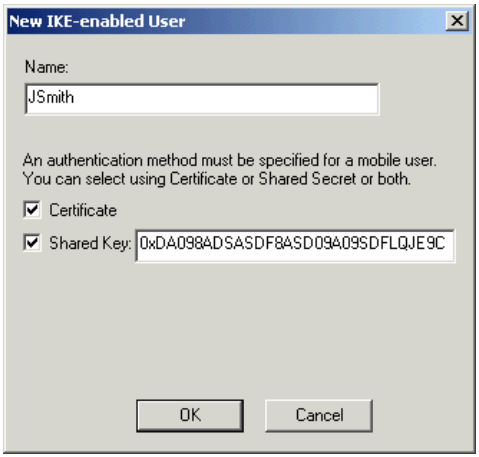


Figure 5-20 IKE-enabled User dialog box

3 In the New IKE-enabled User dialog box, type the **Name** of the VPN Client user (*JSmith*).

4 Select the authentication method(s) this user will use. You can select Certificate, or Shared Key, or both.

- If you select Certificate, you must create an Entrust Certificate and provide it to the user. See the section on configuring certificate authentication in the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide.*
- If you select Shared key, enter a shared key of 20 or more printable characters. Record the shared key so that you can provide it to the VPN Client user.

This example shows the use of both a certificate and s shared key.

5 Click **OK**.

Your new user (JSmith) is automatically entered in the first part of step 1 (see Figure 5-21).

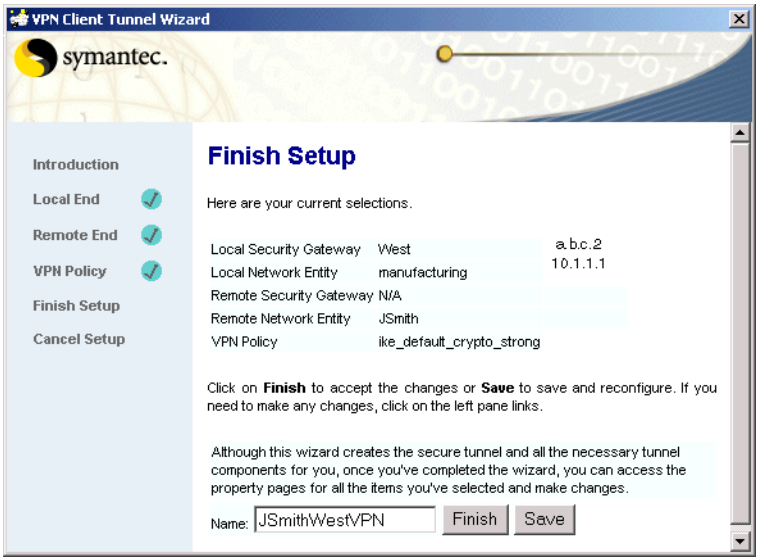

VPN Client Tunnel Wizard
symantec.
Introduction
Local End
Remote End
VPN Policy
Finish Setup
Cancel Setup
Finish Setup
Here are your current selections.
Local Security Gateway West
Local Network Entity manufacturing
Remote Security Gateway N/A
Remote Network Entity JSmith
VPN Policy ike_default_crypto_strong
a.b.c.2
10.1.1.1
Click on Finish to accept the changes or Save to save and reconfigure. If you need to make any changes, click on the left pane links.
Although this wizard creates the secure tunnel and all the necessary tunnel components for you, once you've completed the wizard, you can access the property pages for all the items you've selected and make changes.
Name: JSmithWestVPN
Finish
Save

Figure 5-21 Finish Setup screen: VPN Client Tunnel Wizard

Once you have made your remote VPN Client selection, click the **VPN Policy** link to continue configuring your tunnel. The VPN Policy configuration procedure is the same as in the S2S example. Refer to the steps after the figure **VPN Policy screen: S2S Tunnel Wizard on page 91** to continue.

Chapter 6

Routes and DNS

Routing is the process of choosing a path over which to send packets of information. For the security gateway to function properly, specific routes must be defined in the Routing Tables. Network routes must be configured properly to allow information to move from machine to machine.

This chapter explains how to configure routes and set up the name service using the DNS proxy. Make sure you have a solid working knowledge of DNS before proceeding, as well as a list of the names and IP addresses of all computers at your site, both in front of and behind the Symantec Gateway Security appliance.

The configuration done in this chapter includes only the most basic name service features. Refer to the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for more advanced features.

Setting up routes

Your TCP/IP Protocol must be configured properly for Symantec Gateway Security appliance to work. This includes setting static routes (or default gateways) on your Symantec Gateway Security appliance and your other computers.

Routes are necessary if you have a routed network behind the Symantec Gateway Security appliance. The Symantec Gateway Security appliance must be able to find the appropriate router through which to send packets.

- A routed network has more than one subnet behind the Symantec Gateway Security appliance inside network interface. Other networks are behind routers or gateways.
- A flat network has only one subnet behind the Symantec Gateway Security appliance. There is no router or gateway system behind the appliance.

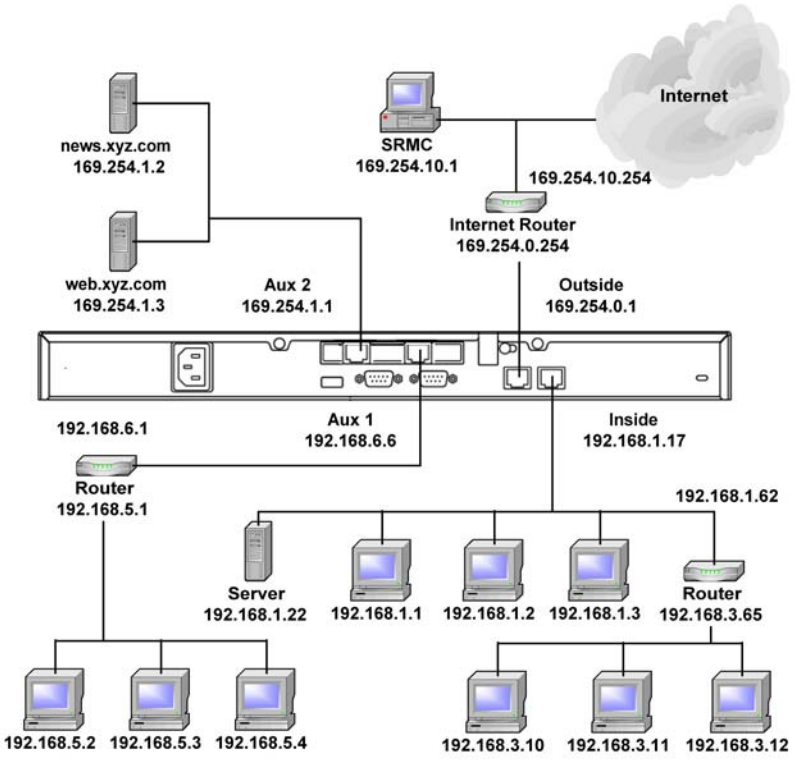


Figure 6-1 A Routed network example

In the example network in Figure 6-1, default route settings for the internal network are as shown in Table 6-1.

Table 6-1 Default route settings

news	169.254.1.2 (SGSA aux1 interface)
web	169.254.1.3 (SGSA aux1 interface)
server	192.168.1.17 (SGSA inside interface)
wkst1 - wkst3	192.168.1.17 (SGSA inside interface)
wkst10 - wkst12	192.168.3.85 (inside router)
wkst13 - wkst15	192.168.5.1 (inside router)
www	169.254.0.1 (Internet router)

Specifying the default gateway

For most installations, the default route will be your Internet router. In the example network shown in Figure 6-1, the Symantec Gateway Security appliance host must have the default route set to 169.254.0.254.

When you first configure the Symantec Gateway Security appliance using the setup wizard, you enter the default gateway information on the first screen. If for some reason, the default gateway was not specified then, you can specify it by accessing the Symantec Gateway Security appliance Properties page.

To specify the default gateway

1. Select the icon of the Symantec Gateway Security appliance you are configuring.
2. From the **Action** menu, select **Properties.**

The **Symantec Gateway Security appliance Properties** page displays

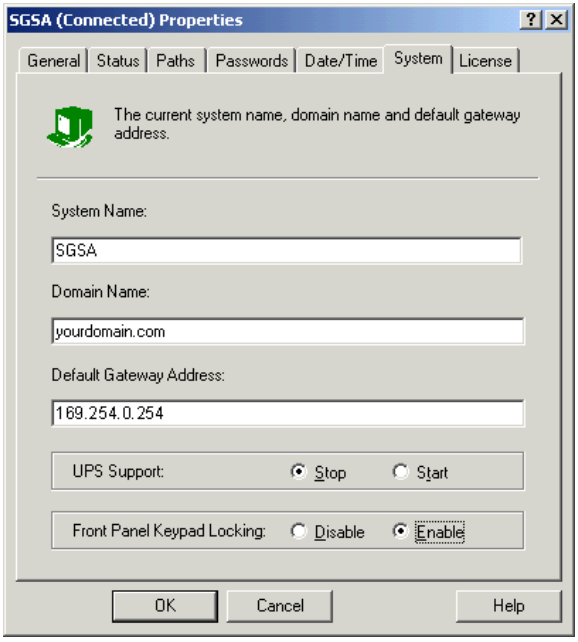


Figure 6-2 Route properties window

3 Select the **System** tab and enter the default gateway information, as shown in Figure 6-2.

4 Click **OK** to save your updated default gateway information.

You must save and reconfigure the Symantec Gateway Security appliance for your changes to take effect.

1 Right click in the left pane.

2 Choose **All Tasks>Save and Reconfigure**.

Creating static routes

Static routes are necessary if you have a routed network behind the Symantec Gateway Security appliance. For the routed network to work properly, the router or routers must be properly configured. Use the `ping` command to check the ability of computers on routed networks to connect to the Symantec Gateway Security appliance. It is recommended that you use contiguous networks to reduce the number of static routes required. The network in Figure 6-1 requires a route for the 192.168.3.0 and 192.168.5.0 networks.

To create a route

1 Select the **Routes** icon, right mouse click and choose **New** > **Route**.

The Route Properties window opens (see Figure 6-3).

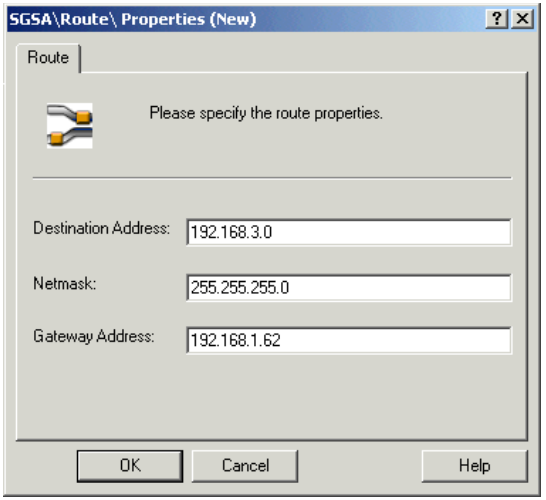


Figure 6-3 Route Properties (New) screen

2 Type the **Destination** network. In our example, it is the network behind the inside router: 192.168.3.0.

3 Type the appropriate netmask. In our example: 255.255.255.0.

4 In the Gateway Address field, type the address of the router.

For example, 192.168.1.62. This is the router address on the same network as the Symantec Gateway Security appliance inside interface.

5 Click **OK** to save route information and close the Route Properties window.

Any connection for an address in the range of 192.168.3.0 to 192.168.3.254 is directed to the router (192.168.1.62).

You would repeat this procedure to create a static route for the 192.168.5.0 subet.

Configure the DNS proxy

The DNS proxy provides a simple way to handle name service at your site. It does not provide private information to outside users.

This chapter uses the `xyz.com` network (shown in Figure 6-1) as a typical example of how to configure the DNS proxy. It includes only basic functionality. The example network has a Symantec Gateway Security appliance that does all the name resolution for this site. There is a protected news server on a service network. The main networks are the private protected machines.

An alternative to using the DNS proxy by itself to provide all name resolution is to use an inside name server for inside name requests. The DNS proxy still deals with outside requests. This is called a dual-level DNS.

Caution: You should understand DNS before attempting to configure the DNS proxy. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide* for information on DNS.

Provide private DNS file address statements

The DNS private entries are stored in the Linux DNS entries `hosts` file, and the public entries are stored in the `hosts.pub` file. Use SRMC to specify the DNS entries as Public or Private. Private machines are intended for use by inside users only. Their names and IP addresses are kept secret from the outside interface to help prevent attack.

You can create the DNS entries using the SRMC DNSD Properties window. For more information, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

To create the DNS entries using SRMC

1. Expand the **Base Components** folder in the SRMC.
2. Select the **DNS Records** icon.

   The existing DNS entries appear in the right pane (see Figure 6-4).

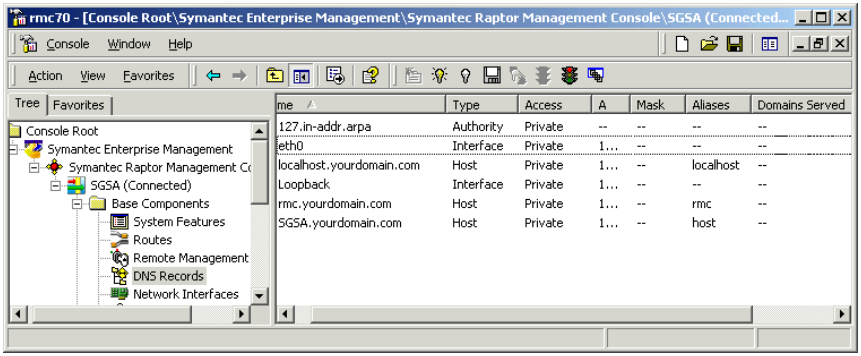


Figure 6-4 SRMC hosts list

3 To create a new host, right click and choose **New** > **Host**.

The **DNS Record** Properties page appears (see **Figure 6-5**).

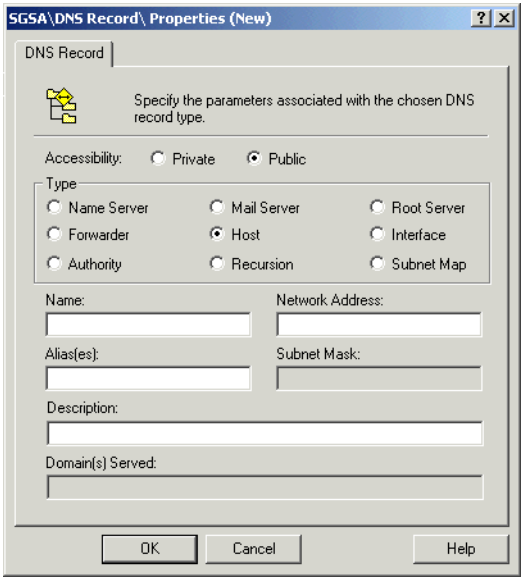


Figure 6-5 DNS Record Properties page

4 Under **Accessibility**, select whether the Host is **Private** or **Public**.

If you select Private, the data you typed is added to the `hosts` file. If you select Public, the data is added to the `hosts.pub` file. (See **Provide**

hosts.pub file information on page 107 for information on the `hosts.pub` file).

5 Under **Type**, select the **Host** radio button if it is not already selected.

When you select a Type, the fields in the DNS Record Property page that require data entry become available.

6 In the **Name** field, type a fully qualified host name.

7 In the **Network Address** field, type the IP address for the host.

8 In the **Alias(es)** field, type the host's nickname(s).

You can type several nicknames at once into this field, separating each by a space.

9 In the **Description** field, type a **Description** and click **OK.**

The information you enter is written to the `hosts` file. The `hosts` file includes lines with an address and name. More than one name can be included for an address.

10 Click **OK** to close the DNS Record Properties page.

The entries for the 192.168.1.0 and 192.168.3.0 subnets in the `hosts` file for the example network in Figure 6-1 would look like this. Items are separated by one or more spaces.

```
192.168.1.17  SymantecGatewaySecurity.xyz.com
    Symantec Gateway Security
192.168.1.22  server.xyz.com        server
192.168.1.1   wkst1.xyz.com
192.168.1.2   wkst2.xyz.com
192.168.1.3   wkst3.xyz.com
192.168.3.10  wkst10.xyz.com
192.168.3.11  wkst11.xyz.com
192.168.3.12  wkst12.xyz.com
```

Note: Aliases are acceptable, as long as every line has a fully qualified host name.

Your `hosts` file should also contain the following line, specifying the localhost (or loopback) address.

```
127.0.0.1   localhost.xyz.com  localhost
```

The `hosts` file is the first place where the DNS proxy looks for an address when the request comes from a private system. You can add any other addresses to this file. For example, you might want to add outside machines from your network, as follows:

```
169.254.1.2    news.xyz.com news
169.254.1.3    web.xyz.com  www
```

You can also add frequently used hosts on the Internet to this file. Doing so can skip several name request steps.

Provide hosts.pub file information

The `hosts.pub` file provides host-to-IP address and address-to-host mappings for *public systems*. These are computers at your site that are intended for use by both inside and outside users.

The `\etc\hosts.pub` file uses the same format as `hosts`. Each line must include an address and a fully qualified name.

The following examples show entries that might appear in the `hosts.pub` file for the sample network in **Figure 6-1**. Again, a fully qualified host name is required on each line.

```
169.254.1.2  news.xyz.com
169.254.1.3  web.xyz.com
169.254.0.1  SymantecGatewaySecurity.xyz.com
```

Unlike information in `hosts`, information on systems in the `hosts.pub` file is available to both public and private networks.

Note: As in `hosts`, aliases are acceptable, as long as every line has a fully qualified host name.

Verify connectivity

On a system on the inside network, use `ping` to check whether your network is set up properly. Verify that you can connect to computers on the Internet and on each of your subnets.

The `ping` command uses Internet Control Message Protocol (ICMP) echo packets to see if you can connect to a computer. You can `ping` using either name or address.

Use `ping` in a command prompt window on your machine running SRMC. The syntax for `ping` is:

```
ping IP address or ping computer name
```

If you `ping` by name, the `ping` utility first attempts to find the address. If it cannot find the address, because of DNS or WINS problems, `ping` responds with "bad IP address." If it finds the address, `ping` proceeds.

If you `ping` by address, `ping` sends a request for a response. If the computer is working and if you can reach it, you receive reply messages. If the computer is down or something is wrong with the network between you and the other computer, `ping` tells you the computer is unreachable or that the request has timed out.

The following section refers to the routed network example in **Figure 6-1** and uses the computer names shown in **Table 6-2**.

Table 6-2 Routed network example computer names

IP address	Computer name
192.168.1.1	wkst1
192.168.1.2	wkst2
192.168.3.12	wkst12

- From a computer behind the appliance, such as `wkst1`in our example, `ping` a computer on each subnet behind the Symantec Gateway Security appliance as follows:

  ```
  ping wkst2.xyz.com
  ```

  ```
  ping wkst12.xyz.com
  ```

Both of these computers should be reachable. If either of these commands fails, try again, using addresses:

```
ping 192.168.1.2
```

```
ping 192.168.3.12
```

If the `ping` command succeeds with the address, you have a name resolution problem.

If they are still unreachable, you have a networking problem. Make sure that `wkst2` and `wkst12` are on and connected to the network. Check the default gateway setting on `wkst1` (it should be set to the inside interface of the Symantec Gateway Security appliance).

If `wkst2` is reachable but `wkst12` is not, your static route from Symantec Gateway Security appliance has not been established or your router is not configured properly. Also, check your default gateway setting on `wkst12`.

If you can not `ping` an address behind a router, `ping` both addresses of the router. If one is reachable but the other is not, you have a routing configuration problem.

- Test the news server with this command:

  ```
  ping news.xyz.com
  ```

- From an internal machine like `wkst1`, `ping` a computer outside your network.

  ```
  ping www.symantec.com
  ```

  The request should return an IP address for the requested name. The `ping` itself will be “timed out” or “unreachable” because `ping` is blocked by the Symantec Gateway Security appliance. However, when the `ping` utility requests an IP address, DNS should be able to find it.

  If `ping` does not get an IP address for the outside name, you have a problem with outside name service.

  If you cannot receive an IP address for an outside name, attempt the same `ping` command from an outside machine (`www.xyz.com` in our example). If it does not work from there, the problem is more likely in your Internet router or your ISP's name server.

  Check to see that your default gateway is set properly.

Chapter 7

Management Console

The Symantec Raptor Management Console (SRMC) is the graphical user interface for managing and monitoring all functions on the Symantec Gateway Security appliance.

Once you have connected to the Symantec Gateway Security appliance, you can use the SRMC to edit information you entered during the initial Symantec Gateway Security appliance configuration, such as passwords and license key data, and all other configuration tasks. Because the communications between the SRMC and the Symantec Gateway Security appliance are encrypted, you can securely manage the appliance from a remote location.

You can manage several appliances from a single SRMC and also manage a single appliance from several SRMCs. You can also manage a mixture of Symantec Gateway Security appliances, Symantec Enterprise Firewalls, and Symantec Enterprise VPNs from the same SRMC.

The Symantec Gateway Security appliance comes with an additional management utility called SRL (Secure Remote Login), which offers an encrypted secure communication to the Symantec Gateway Security appliance at the command line level, to allow remote access to the operating system if needed. The SRMC is designed to provide access to all needed operating system configurations. See **Use secure remote login on page 128** for further details on SRL.

Monitor Symantec Gateway Security appliance

Before you move into more advanced management functions, it is important to understand the monitoring capabilities of the Symantec Gateway Security appliance. The *Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide* deals with monitoring in detail.

The Logfiles window allows you to view logfiles that contain information about the Symantec Gateway Security appliance's operation. To access this window, click on **Logfiles** in the SRMC root directory.

Table 7-1 lists a few messages you may encounter right after setup. For a full list of messages, see the log file messages appendix of the *Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide*. A number of common problems are discussed in depth in Knowledge Base, accessible from the Symantec Customer Service Support website at `http://www.symantec.com/techsupp/`.

Table 7-1 Setup

Number	Message	Explanation
120	TYPE Info: informational_message	This message logs information, such as, license status and DNS problems.
121	statistics: duration=(seconds) user=(user) auth=(auth type) sent=(amount) rcvd=(amount) srcif=(source interface) src=(source/port) dst=(dest/port) op=(option) arg=(file) result=(result) proto=(protocol) notes	This message logs statistics about a connection. Elements are optional but occur in this order. Info 121 can be used by custom applications for accounting.
501	access from incoming to outgoing (rule): (time period)	Suspicious Activity Monitoring has been triggered. While heavy access can indicate an attack, soon after you install, it is more likely that your thresholds are too low on heavily used services (http in particular).

Table 7-1 Setup

Number	Message	Explanation
516	CPU Temperature is low/high 300 MHz appliance: Normal Range 0° to 70° 450 MHz appliance: Normal Range 0° to 80°	This message indicates that the Symantec Gateway Security appliance temperature is slightly lower or higher than the normal operating temperature.
616	CPU Temperature is too low/high	This message signals that the Symantec Gateway Security appliance temperature has reached a critical level.

Managing passwords

Once the Symantec Gateway Security appliance is connected (see **Connect to Symantec Gateway Security appliance on page 54**), you can use SRMC to make changes to the information you entered and the passwords you made note of during the initial setup procedure.

Note: Remember to document and save your passwords. Passwords for the SRMC, Root, and Secure Remote Login (SRL) may be requested during future configuring of the Symantec Gateway Security appliance. You will need to know these passwords to do a configuration Backup and Restore. During the Restore process, the original SRMC password is restored. The Root and SRL passwords are not reset to their original state.

Remote management password

You can change the Symantec Gateway Security appliance's remote SRMC password from the Remote Management Password property page.

To specify a SRMC password

1. Expand the **Base Components** folder.
2. Select the **Remote Management Passwords** icon in the left pane.
3. Right click and choose **New** > **Remote Management Password**.

   The Remote Management Password Properties page opens (see **Figure 7-1**).

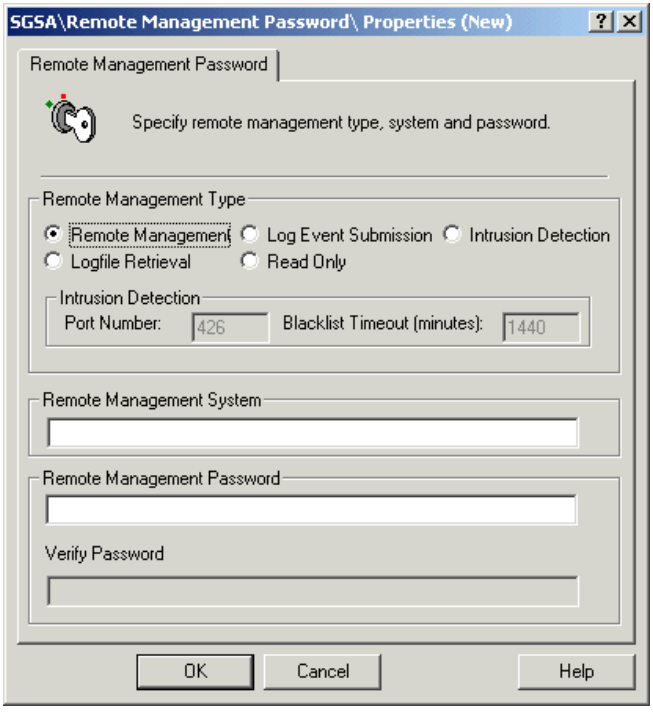


Figure 7-1 Remote management passwords

4 In the **Type** section, select the **Remote Management** radio button, if it is not already selected.

5 In the **Remote Management System** field, type the **IP address** of the Windows NT system running the managing SRMC.

6 Type your new password into the **Remote Management Password** field.

7 Type the new password again into the **Verify Password** field.

8 Click **OK**.

Root and secure remote login passwords

You can change the Symantec Gateway Security's root password and your Secure Remote Login (SRL) password from the System Properties page.

To change the Root and SRL passwords

1. Connect to the Symantec Gateway Security appliance (see **Connect to Symantec Gateway Security appliance on page 54**).
2. Select the icon of the connected appliance in the left pane. Right click and choose **Properties**. The appliances Properties page opens (see **Figure 7-2**).

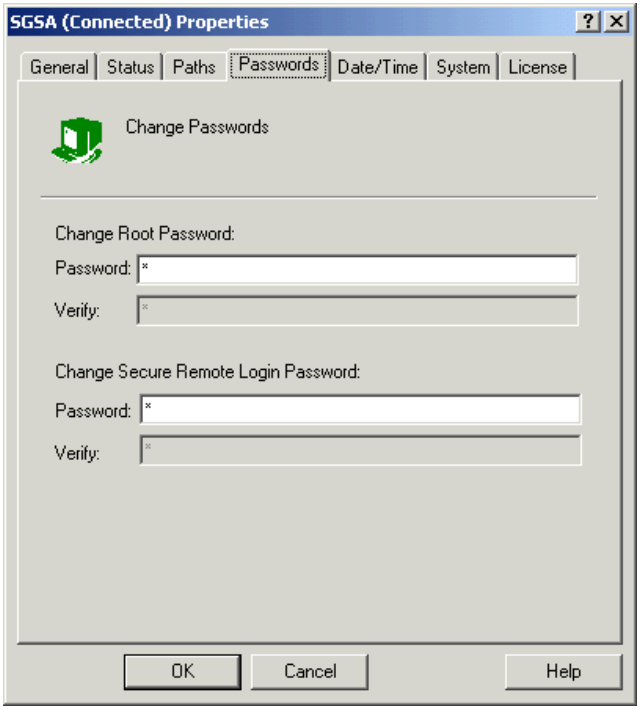


Figure 7-2 System Properties page, Password tab

3. Select the **Passwords** tab.

   You can change your Root password and/or your SRL password here.
4. Using the Root password or SRL password section of the screen. in the **Password** field, type a new password.
5. In the **Verify Password** field, type the new password again.

6 Click **OK**.

See **Use secure remote login on page 128** for instructions on Secure Remote Login. See the *Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide* for further information.

Change system settings

You can change the Symantec Gateway Security appliance's system settings from SRMC.

To change the system settings

1 Connect to the Symantec Gateway Security appliance (see **Connect to Symantec Gateway Security appliance on page 54**).

2 Select the icon of the connected appliance in the left pane.

3 Right click and choose **Properties**.

The appliance's properties page opens.

4 Select the **System** tab (see **Figure 7-3**).

Here you can change the Symantec Gateway Security appliance system name, the domain name, and the default gateway address. You can also select to use UPS (Uninterruptible Power Supply) support, and to enable or disable front keypad locking. See **Front panel keypad locking on page 129** for more information.

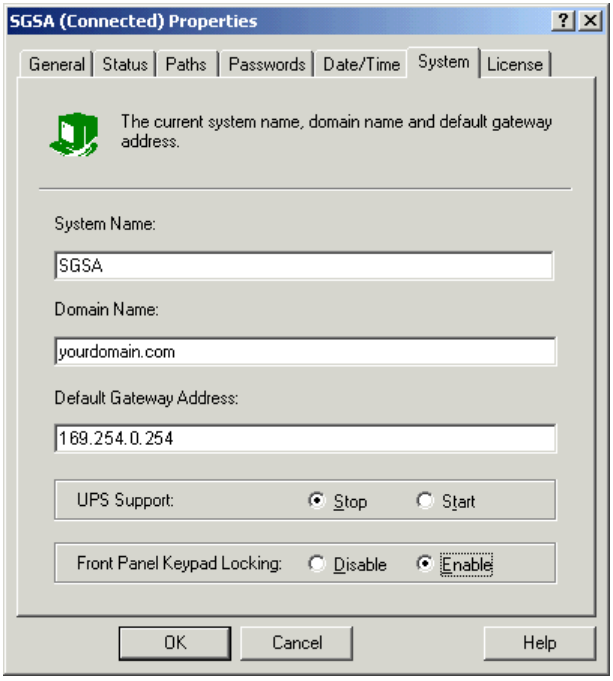


Figure 7-3 System settings

5 Make any necessary changes.

6 Click **OK**.

You must save and reconfigure the Symantec Gateway Security appliance for your changes to take effect.

7 Right click in SRMC.

8 Select **All Tasks** > **Save and Reconfigure**.

Change the date and time

You can change the Symantec Gateway Security appliance's date and time through the SRMC.

To change the date and time

1 Connect to the Symantec Gateway Security appliance (see **Connect to Symantec Gateway Security appliance on page 54**).

2 Select the appliance system icon of the connected appliance in the left pane.

3 Right click and choose **Properties**.

The appliance's properties page opens.

4 Select the **Date/Time** tab (see Figure 7-4).

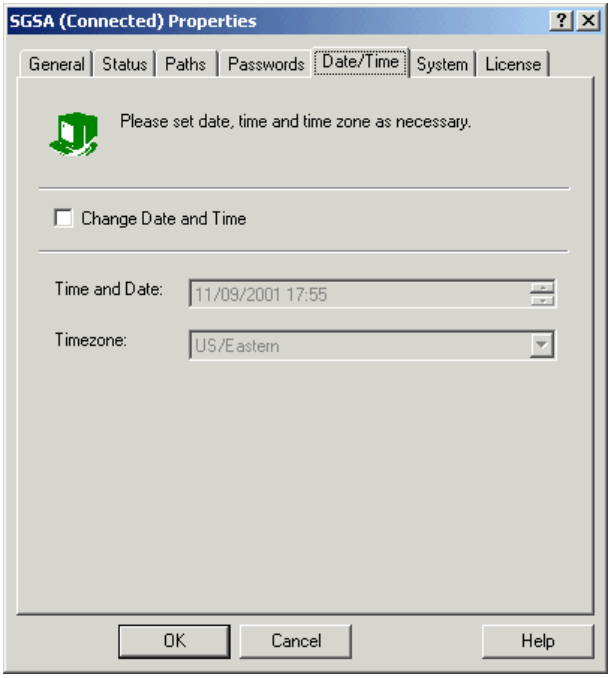


Figure 7-4 Change date and time

5 Check the **Change Date and Time** checkbox to change the current settings.

6 From the **Time and Date** and **Timezone** pull-down fields, choose the appropriate settings.

7 Click **OK** when finished.

Changes take effect immediately.

Define a license key

If necessary, you can enter a license key for the first time or change the current Symantec Gateway Security appliance license key through SRMC from the license tab of the appliance's properties page. For further license key information, see **Get your license key on page 45**.

To enter or change your license key

1 Select the appliance's icon in the left pane.

2 Right click and choose **Properties** to display the appliance's properties page.

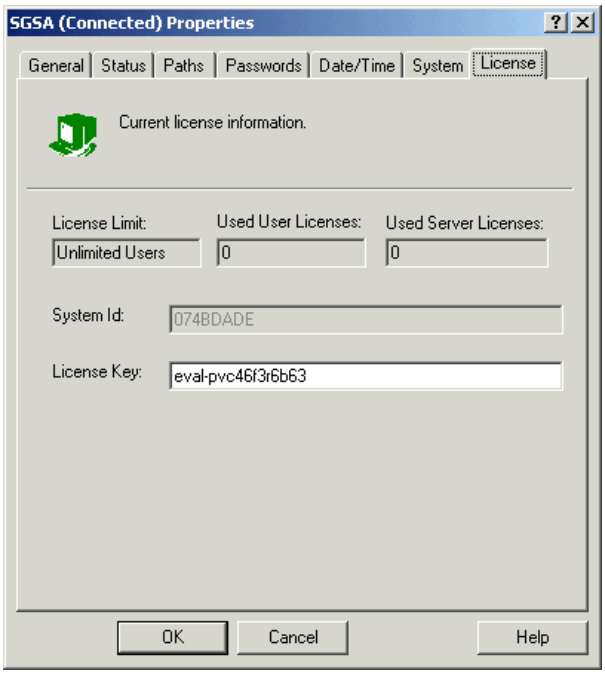


Figure 7-5 Type a license key

3 Select the **License** tab (see Figure 7-5).

4 Enter a new Symantec Gateway Security appliance license key or, if you have a 30 day non-licensed copy, enter a license key for the first time.

5 Click **OK**.

6 To save your new key, right click in SRMC, and select **All Tasks** > **Save and Reconfigure**.

7 To make the license change take effect, reboot the Symantec Gateway Security appliance.

Perform a system shutdown from SRMC

From the SRMC **All Tasks** menu, you can remotely perform Symantec Gateway Security appliance system shutdowns.

To shutdown from SRMC

1 Right mouse click from within SRMC and select **System Shutdown** from the **All Tasks** menu (see Figure 7-6).

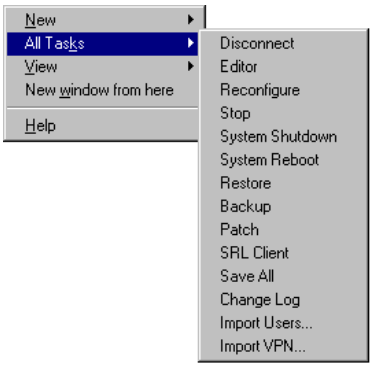


Figure 7-6 SRMC All Tasks menu

2 You are asked to confirm this shutdown.

A System Shutdown brings down the Symantec Gateway Security appliance software, the Linux OS, and all its applications. The appliance remains powered on, but no software is running.

3 It is safe to turn the Symantec Gateway Security appliance off when the LCD display reads "PLEASE SWITCH POWER OFF NOW".

4 You must now power cycle the appliance to bring it back up.

Perform a system reboot from SRMC

From the SRMC **All Tasks** menu, you can remotely perform system reboots.

To reboot from SRMC

1 Right click from within SRMC and select **System Reboot** from the **All Tasks** menu (see Figure 7-6).

2 Confirm this reboot.

A System Reboot restarts the Symantec Gateway Security appliance software. The Linux OS and all its applications are brought down and then restarted.

Back up configuration files

From the SRMC **All Tasks** menu, you can perform manual system backups of your configuration files.

Configuration files are stored the Symantec Gateway Security appliance. Back up files are stored on the SRMC machine. Backed up files are identified by hostname, date, and time, with an `.rfwcfg` extension.

For example, Symantec Gateway Security-2002-March-15-13-51-48.rfwcfg

To do a manual configuration file backup

1 Right click from within SRMC and select **Backup** from the **All Tasks** menu.

The Backup dialog box is displayed. (see **Figure 7-7**).

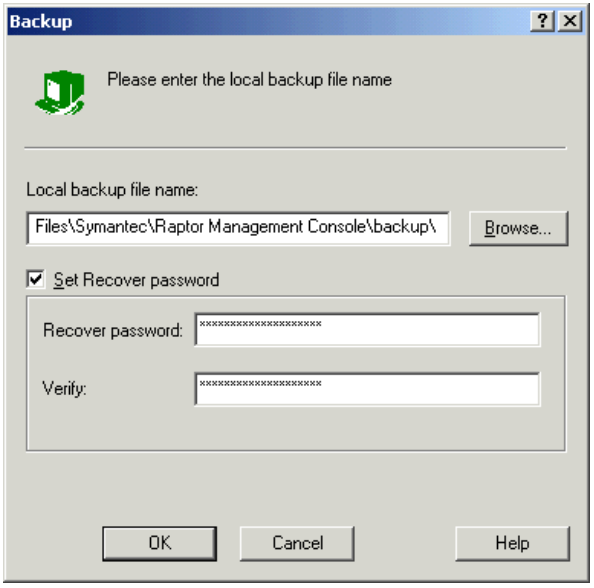


Figure 7-7 Backup property page

2 From the **Local backup file name** field, click **Browse** to display the open Saved System Configuration dialog box. This opens to the default location for backup files:

\Program Files\Symantec\Raptor Management Console\backup

When you enter a filename and click **Save,** the file name is placed in the field.

You can also enter the path and a file name for the backup directory into the field. The file name must have the extension `.rfwcfg`. If the directory does not exist, you are asked if you want to create it.

3 Optionally, you can select the **Set Recover password** check box and enter a password. This will allow you to decrypt your keys files if you copy these backed up files to another Symantec Gateway Security appliance with a different system name (see **Restore configuration files on page 124**).

Note: If you do not enter a password, you cannot restore backed up configuration files to another Symantec Gateway Security appliance. You can only restore them on the same machine.

Restore configuration files

From the SRMC **All Tasks** menu, you have the option of restoring backed up configuration files to your Symantec Gateway Security appliance or to another Symantec Gateway Security appliance. If you originally backed up these files using a password to restore and decrypt the keys files on a another machine, you must enter this same password on the new machine when you restore.

Caution: This procedure assumes that the new machine has the same IP addresses and hostname as the original. Otherwise, you may have to edit configuration files by hand (using SRL) after restoring them to the new machine.

To restore backup configuration files to your Symantec Gateway Security appliance

1 Right mouse click from within SRMC and select **Restore** from the **All Tasks** menu to display the Restore Property window (see Figure 7-8).

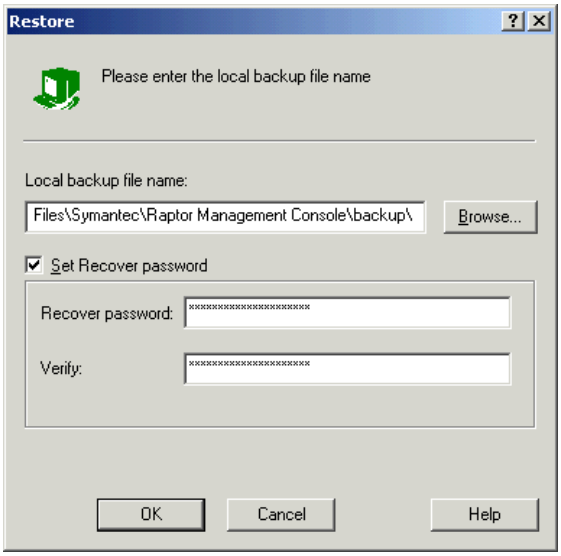


Figure 7-8 Restore property page

2 From the **Local backup file name** field, use the **Browse** button to locate the backed up *.rfwcfg file you created.

3 If you typed a recovery password when you backed up the files on the original machine, select the **Set Recover password** check box and type the same password here to decrypt your secret keys on the second machine.

Note: If you did not enter a password when you originally backed up these files, you can restore the configuration files to the same machine but you cannot successfully restore the files to another machine.

---

4 Click **OK.**

Apply patches to the Symantec Gateway Security software

Patches or hot fixes may be provided for your existing Symantec Gateway Security software. The **Patch** option, available from the SRMC **All Tasks** menu (see Figure 7-6), lets you "push" a patch from the SRMC machine to the Symantec Gateway Security appliance.

To apply a patch

1 Once you have downloaded the patch (.tgz file) from the Symantec Web site to your SRMC machine, you can select **All Tasks** > **Patch** from within SRMC.

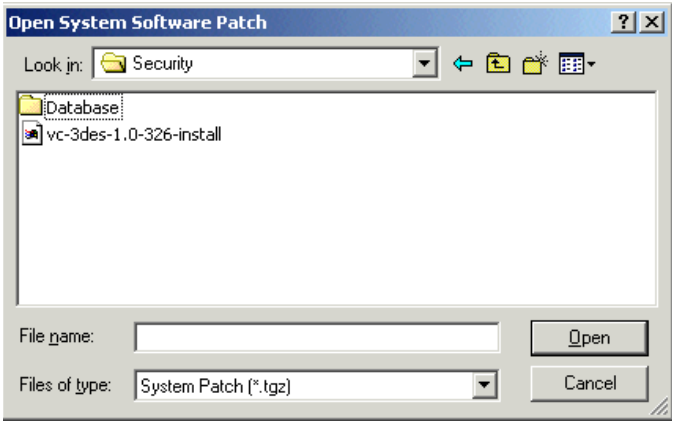


Figure 7-9 Open System Software Patch page

2 The SRMC prompts you to browse to the patch on your local system.

3 When you locate the patch, select **Open**.

The patch unpacks and installs to the Symantec Gateway Security appliance.

Note: Once the patch or hot fix is applied, the Symantec Gateway Security appliance automatically reboots and the SRMC disconnects from the appliance.

Manage log files

When a logfile exceeds a certain size (default 200MB), the system automatically starts another logfile by running the `Changelog` command. This prevents a single logfile from exhausting the available disk space. Through SRMC, you can perform a manual Changelog command on the Symantec Gateway Security system to rollover the current logfile to the `/oldlogs` directory. For more detailed information on Changelog, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Guide,* provided as a PDF file.

To perform a manual ChangeLog command:

1 Select **All Tasks** > **ChangeLog** from within SRMC (see **Figure 7-10**).

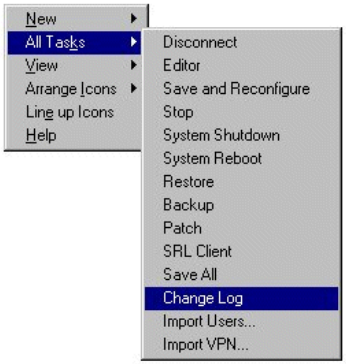


Figure 7-10 ChangeLog menu

2 The current logfile is placed in the `/oldlogs` directory and named according to the SRMC logfile dating convention.

For example `2002315` (Mar. 15, 2002). A new logfile is then started.

Add SRMCs

The appliance can be managed by more than one SRMC, although not at the same time. To configure remote management by another SRMC, follow the instructions in **Managing passwords on page 114**. Be sure to type the IP address of the new Remote Host in the appropriate field.

You can then connect to this appliance with an SRMC with that specified address. Type the appropriate hostname and password into the login window.

Use secure remote login

Secure Remote Login lets a user on a machine with SRMC to login to the Symantec Gateway Security appliance and review system files, reboot the machine, or perform other troubleshooting or debugging tasks that are outside of normal appliance operations. All remote traffic is encrypted. You must use the SRMC version of Tera Term Pro, and not the standalone version.

To make an SRL connection from SRMC to the Symantec Gateway Security system

1 From your managing SRMC system, right click and choose **All Tasks** > **SRL Client** to display the Tera Term Pro window logon dialog box (see *Figure 7-11*).

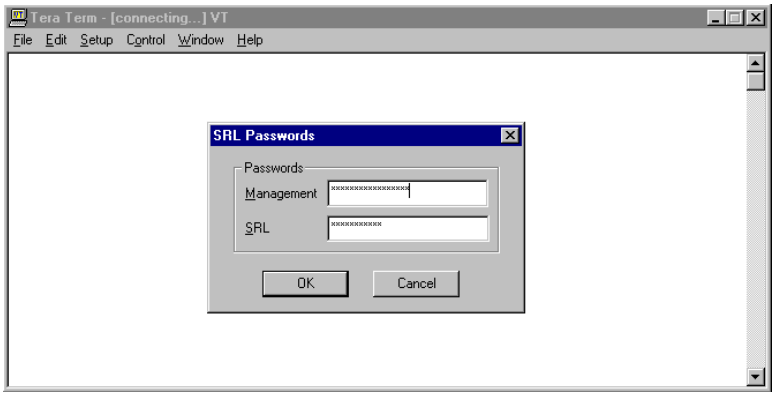


Figure 7-11 Tera Term Pro window

2 Enter your SRMC password in the **Management** field.

3 Enter your SRL password in the **SRL** field.

You need this password to establish a secure connection. The Symantec Gateway Security appliance displayed this password to you during the initial setup procedure. You can change the SRL password through SRMC as described in Managing passwords on page 114.

4 Click **OK**.

Once connected through SRL, you can securely perform any necessary administrative functions on the Symantec Gateway Security appliance.

Front panel keypad locking

Locking the Symantec Gateway Security appliance provides additional security against personnel who should not have access privileges to the appliance. If the front panel is locked, only individuals with knowledge of the Root System Password can disable the lock in order to continue working with the front panel.

To enable locking

1. From the SRMC, select the Symantec Gateway Security appliance icon and right click.
2. Choose **Properties** to display the appliance's Properties page.
3. Select the **System** tab.
4. Beside Front Panel Keypad Locking, choose the **Enable** radio button to lock the front keypad (see Figure 7-12).

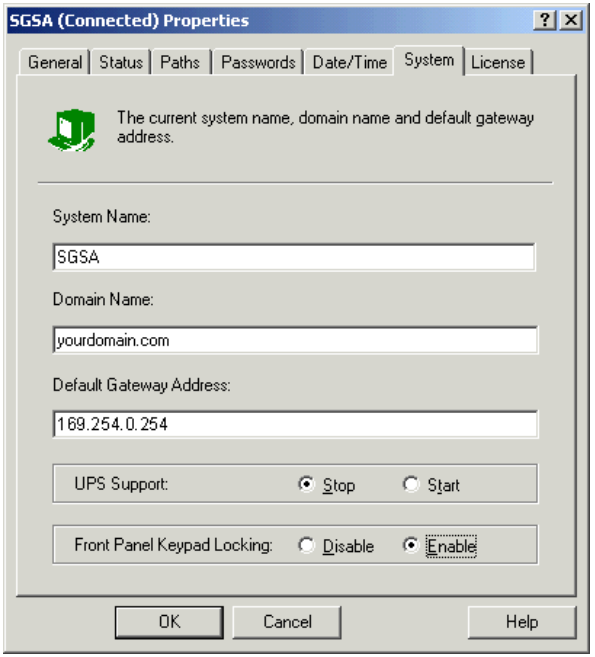


Figure 7-12 Enabling keypad locking

5. Click **OK**.
6. **Save** and **Reconfigure**.

Use a locked keypad

To use a locked keypad

1. When you press an arrow key on the appliance front panel with the keypad locked, the root password prompt displays. Type the root password that was provided during setup (see **Step 9 on page 40**).
2. To enter your Password, use the keypad Up (^) and Down (v) arrow buttons on the appliance front panel to scroll through the alphabet characters. When your Password character appears in the brackets [ ], press the right arrow (>) button on the keypad to make your selection and go on to select your next character using the same process.

   Passwords are limited to 8 lowercase alpha (a-z) characters only.

   Note: If you type an incorrect character, you can either press the Cancel button ('S') or you can go back using the left arrow (<) button. Your selections will be erased to the point at which you want to make your correction.

   ---

3. Once you have correctly typed your Password, press the **E** button. You now have access to the locked keypad.

   Once Locking is enabled, the appliance automatically locks after five (5) minutes of keypad inactivity.

Chapter 8

Intrusion Detection System (IDS)

The IDS technology available with the Symantec Gateway Security appliance provides dynamic network intrusion detection that transparently examines network traffic to instantly identify, log, and terminate unauthorized use, misuse, and abuse of computer systems by internal saboteurs and external hackers. The IDS compares individual packets from the firewall to a file of attack signatures.

An attack signature is a set of rules that identifies an attacker's attempt to exploit a known operating system or application vulnerability. Both the header and the payload information for each packet are examined to distinguish attacks from legitimate traffic. In addition, with IDS, the appliance detects atomic signatures.

When the IDS detects an attack, it creates a log entry in the log file on the Symantec Remote Management Console (SRMC). With IDS, you can set notification options to notify designated people in response to different levels of alert messages detected. For more information, see **IDS notifications on page 147**.

IDS Components folder

The IDS Components folder consists of three branches – Configuration, Reports, and Monitoring.

Configuration

The Configuration option allows you to configure:

- Signatures

  The attack signatures file shipped with the appliance contains signatures that detect the most common network attacks, such as Denial of Service and Buffer Overflow.

  The IDS component can be configured to detect attacks by signature name, then treat them as gated or non-gated signatures.

- LiveUpdate

  IDS LiveUpdate allows you to update the selected appliance with an updated attack signatures file that contains the most current IDS attack signatures.

For more information, see **Configuring IDS Signatures on page 134** and **Using LiveUpdate to update attack signatures on page 139**.

Reports

The Reports option allows you to generate two types of reports.

- The Executive Summary reports provide a high-level overview of the number and severity level of attacks seen during a specified time period (daily, weekly, or monthly). Executive Summary reports are a good way to take periodic snapshots of your overall network security.
- The Configuration report provides the current configuration of each attack signature, along with configuration information for LiveUpdate for the selected appliance.

For more information, see **IDS Reports on page 145**.

Monitoring

The Monitoring option provides information on all network attack attempts detected by the IDS component. As the IDS component detects attacks, that information is written to a log file, which is accessed through the SRMC.

Click the Alerts icon in the SRMC Tree to see the list of files available. You can set up a filter to sort through the data collected in a logfile. This feature can be very handy if you want to locate information on attacks of specific severity levels in large logfiles. For more information about viewing alerts, see **Viewing IDS Alerts in the IDS Alerts Viewer on page 142**.

The alerts list has the same structure as system logfiles, which can be viewed by opening the Monitoring Controls folder in the left pane and choosing the Logfiles option. For more information about system logfiles, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

Configuring the IDS component

The IDS component is enabled or disabled during the initial appliance setup. The initial default is for the IDS component to be enabled. For more information, see **Setup wizard on page 56**.

After the initial appliance setup, you can enable or disable the IDS component in the SRMC. For more information, see the following section **Enabling/Disabling the IDS component**.

Because the Firewall/VPN sends packets to the IDS, the Firewall/VPN must be enabled for IDS to function.

Initially all signatures are enabled for detection by default. The gated option is turned on or off as appropriate for each signature. You can configure detection and gating options at the signature level in the SRMC.

Enabling/Disabling the IDS component

You can enable or disable the IDS component in the SRMC.

To enable or disable the IDS component

1. Expand the **Base Components** branch.
2. Click the **System Features** icon.
3. In the right pane, double click the Intrusion Detection System component.
4. In the IDS Properties window, check **Enable Intrusion Detection System** if you want to enable IDS attack detection; uncheck the check box if you want to disable IDS attack detection.
5. Click **OK**.

Configuring IDS Signatures

You can specify the signatures that you want the IDS to detect by enabling and disabling signatures, then marking each enabled signature as either gated or non-gated in the Signature List.

When a signature marked as gated is detected by the IDS, the packets associated with that attack are not allowed to pass through the IDS engine and an entry is written to the logfile. When non-gated signatures are detected, the packets associated with that attack are allowed to pass through the IDS engine and an entry is logged to the logfile.

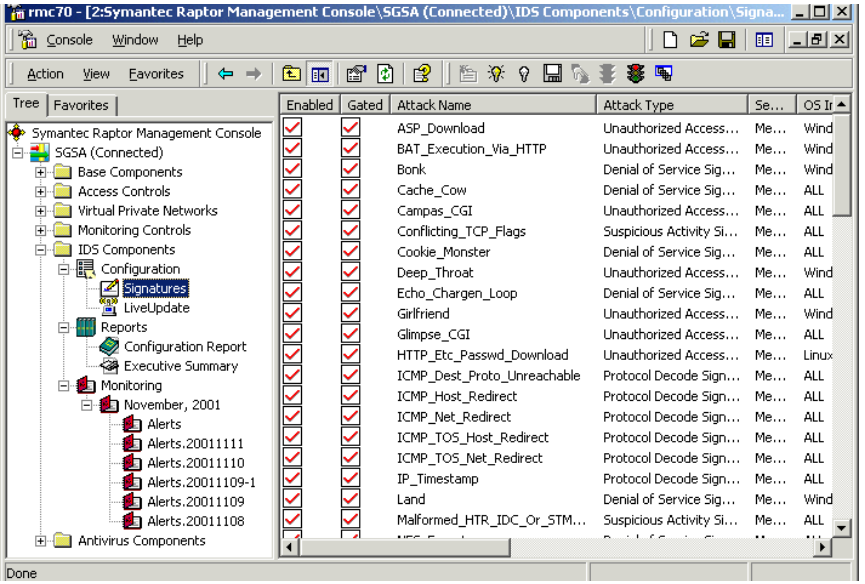
In addition, you can filter the Signature List to view signatures by attack type, operating system, or severity.

Viewing the Signature List

To view the Signature List

1. In the left pane, expand the **IDS Components** folder, and then expand the **Configuration** branch.
2. Click **Signatures**.

   All available signatures appear in the right pane.



A checkmark in the Enabled column for the attack name indicates that the signature is enabled for detection. A checkmark in the Gated column for the attack name indicates that the signature is to be gated upon detection.

You can filter the signatures in the list. For more information, see the following section **Filtering signatures**.

Filtering signatures

You can filter your view of detectable attack signatures by attack type, operating system, and/or severity.

To filter signatures by attack type

1 In the left pane, expand the **IDS Components** folder, and then expand the **Configuration** branch.

2 Click **Signatures**.

All available signatures appear in the right pane.

3 Right click, then click **Filter**.

4 On the **Attack Type** tab, click **Display Selected** to enable the attack type check boxes.

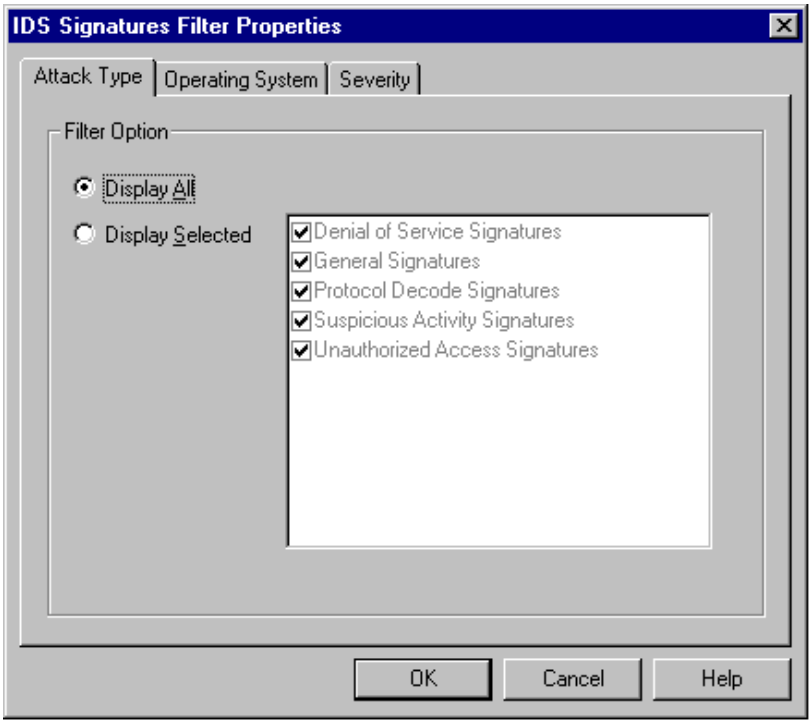


Figure 8-1 IDS Signatures Filter Properties Attack Type page

5 Check the check boxes for the attack types that you want to view in the Signature List.

6 Click **OK**.

All signatures of the selected attack types appear in the right pane.

Note: If no signatures match the selected filter criteria, a message appears in the right pane.

To filter signatures by operating system

1 In the left pane, expand the **IDS Components** folder, and then expand the **Configuration** branch.

2 Click **Signatures**.

All available signatures appear in the right pane.

3 Right click, then click **Filter**.

4 On the **Operating System** tab, click **Display Selected** to enable the operating systems check boxes.

5 Check the check boxes for the operating systems that you want to view in the Signature List.

6 Click **OK**.

All signatures that are affected by the selected operating systems appear in the right pane.

To filter signatures by attack severity

1 In the left pane, expand the **IDS Components** folder, and then expand the **Configuration** branch.

2 Click **Signatures**.

All available signatures appear in the right pane.

3 In the right pane, right click, then click **Filter**.

4 On the **Severity** tab, click **Display Selected** to enable the severity check boxes.

5 Check the check box for each severity level that you want to view in the Signature List.

6 Click **OK**.

All signatures of the selected severity appear in the right pane.

Specifying which signatures the IDS detects

You can specify the signatures that you want the IDS to detect.

To specify the signatures that the IDS detects

1 In the left pane, expand the **IDS Components** folder, and then expand the **Configuration** branch.

2 Click **Signatures**.

All available signatures appear in the right pane. A checkmark in the Enabled column for the attack name indicates that the signature is enabled for detection.

You can select multiple records in the list.

- To select consecutive records, click the first item, press and hold down SHIFT, then click the last item.

- To select records that are not consecutive, click the first item, press and hold down CTRL, then click each item.

3 Right click, then click **Properties**.

4 In the Properties window, check the **Enabled** checkbox to enable all selected signatures. To disable the selected signatures, uncheck the Enabled check box.

5 Click **Apply**.

Signature configuration changes are saved in memory on the SMRC, though the Symantec Gateway Security appliance does not detect signatures based on this configuration until you save and reconfigure.

To save and reconfigure

- Click **Save and reconfigure** on the toolbar, or right click in the left pane and choose **All Tasks**>**Save and Reconfigure**.

Marking a signature as gated or non-gated

You can select the signatures that you want to be gated or non-gated. The gated option can be specified for signatures that are enabled.

To gate a signature

1 In the left pane, expand the **IDS Components** folder, and then expand the Configuration branch.

2 Click **Signatures**.

All available signatures appear in the right pane. A checkmark in the Enabled column for the attack name indicates that the signature is enabled for detection; a checkmark in the Gated column for the attack name indicates that the signature is to be gated upon detection.

You can select multiple records in the list.

- To select consecutive records, click the first item, press and hold down SHIFT, then click the last item.
- To select records that are not consecutive, click the first item, press and hold down CTRL, then click each item.

3 Right click, then click **Properties**.

4 In the Properties window, check the Gated checkbox to gate all selected signatures upon detection. If the selected signatures should not be gated upon detection, uncheck the Gated check box.

5 Click **Apply**.

Signature configuration changes are saved in memory on the SMRC, though the Symantec Gateway Security appliance does not gate or not gate signatures based on this configuration until you save and reconfigure.

To save and reconfigure

- Click **Save and reconfigure** on the toolbar, or right click in the left pane and choose **All Tasks>Save and Reconfigure**.

Viewing additional information for a signature

You can view additional information for each signature that the Symantec Gateway Security appliance can detect in the Signature List. You can also view this information for each alert displayed in the IDS Alerts Viewer. That information includes the attack name, severity, attack type, short description, OS impacted by the attack, and any additional information for that attack signature.

To view additional information for a signature

- In either the Signature List or the IDS Alerts viewer, double click a signature.

Using LiveUpdate to update attack signatures

The IDS LiveUpdate feature allows you to update the selected Symantec Gateway Security appliance with a file that contains the most current IDS attack signatures. This file can contain updates to existing signatures as well. To ensure that you have the most current protection, you should regularly update the attack definition files used by the IDS of the Symantec Gateway Security appliance. Updating the attack definition files ensures that the IDS is looking for the most recent attacks. If your attack definition files are outdated, newer attacks may go undetected.

You can either schedule LiveUpdate to run automatically, or run LiveUpdate on demand (manually) for each appliance connected to the SRMC.

When LiveUpdate is run, the most current IDS attack signatures and an updated help file that contains the signature definitions are downloaded from the LiveUpdate server to the appliance. New signatures are added to the signature list and updated signatures replace existing signatures. Any configuration options set for the updated signatures are retained. All new signatures are turned on by default. The gated option is turned on or off as appropriate for each signature.

An Internet connection is required for LiveUpdate.

For more information, see **Configuring IDS Signatures on page 134**.

Scheduling LiveUpdate

You can schedule LiveUpdate to run on an appliance at the same time every day, at the same time on a specific day every week, or at the same time on the same day of every month.

To schedule LiveUpdate for the IDS

1. In the left pane, expand the **IDS Components** branch, and then expand the **Configuration** branch.
2. Click the **LiveUpdate** node.

   The information for the last LiveUpdate session appears in the right pane.
3. Double click the entry in the right pane.

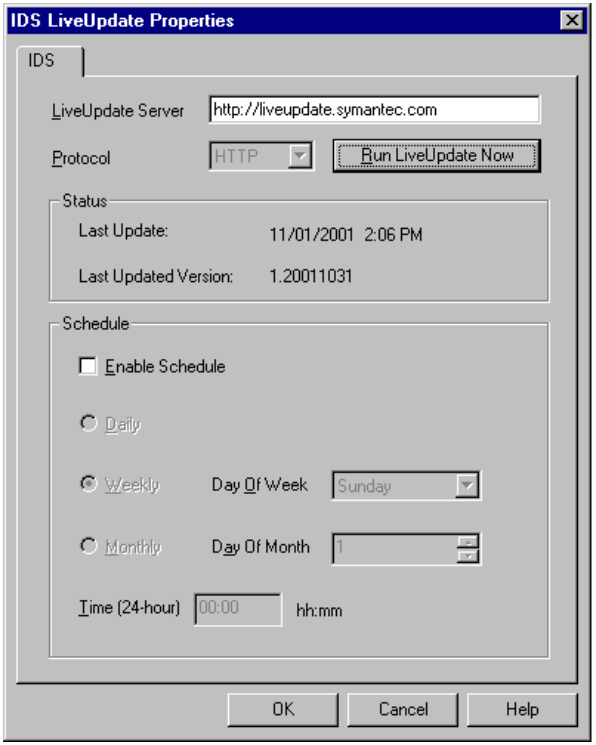


Figure 8-2 IDS LiveUpdate Properties page

4. In the IDS LiveUpdate Properties page, verify that the **LiveUpdate Server** field is pointing to the correct server; change if necessary.
5. Check **Enable Schedule** if it is not already checked.

6 Do one of the following:

- Click **Daily** if you want LiveUpdate to run every day. Then, enter the time to run LiveUpdate.
- Click **Weekly** if you want LiveUpdate to run at the same time on a specific day of every week. Select the day of the week, then enter the time to run LiveUpdate.
- Click **Monthly** if you want LiveUpdate to run at the same time on a specific day of every month. Select the day of the month, then enter the time to run LiveUpdate.

7 Click **OK**.

The LiveUpdate scheduler configuration is saved in memory on the SMRC, though the Symantec Gateway Security appliance does not activate the scheduler until you save and reconfigure.

To save and reconfigure

- Click **Save and reconfigure** on the toolbar, or right click and choose **All Tasks>Save and Reconfigure**.

Running LiveUpdate on demand

You can run LiveUpdate manually at any time to update attack definition files.

To run LiveUpdate on demand

1 In the left pane, expand the **IDS Components** branch, and then expand the **Configuration** branch.

2 Click the **LiveUpdate** node.

The information for the last LiveUpdate session appears in the right pane.

3 Double click the entry in the right pane.

4 In the IDS LiveUpdate Properties window, verify the entry in the LiveUpdate Server field; change if necessary.

Note: If you change the server address, you must save this information before you proceed with step 5. After changing the server address, click **OK** to close the IDS LiveUpdate Properties page, then click **Save and Reconfigure** on the toolbar. Open the property page again, and then proceed with step 5.

---

5 Click **Run LiveUpdate Now**.

A message notifies you that LiveUpdate has been run successfully.

6 Click **OK** in the LiveUpdate status window to close the LiveUpdate Properties page.

Disabling the LiveUpdate scheduler

You can disable the LiveUpdate scheduler at any time.

To disable the LiveUpdate scheduler

1 In the left pane, expand the **IDS Components** branch, and then expand the **Configuration** branch.

2 Click the **LiveUpdate** node.

The information for the last LiveUpdate session appears in the right pane.

3 Double click the entry in the right pane.

4 In the IDS LiveUpdate Properties window, uncheck **Enable Schedule**.

5 Click **OK**.

Viewing IDS Alerts in the IDS Alerts Viewer

IDS attacks are logged in the logfile and appear in the IDS Alerts Viewer. IDS alerts and other informational messages can appear in the main Logfile Viewer if the events are not filtered out of the view.

For more information about the main Logfile Viewer, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

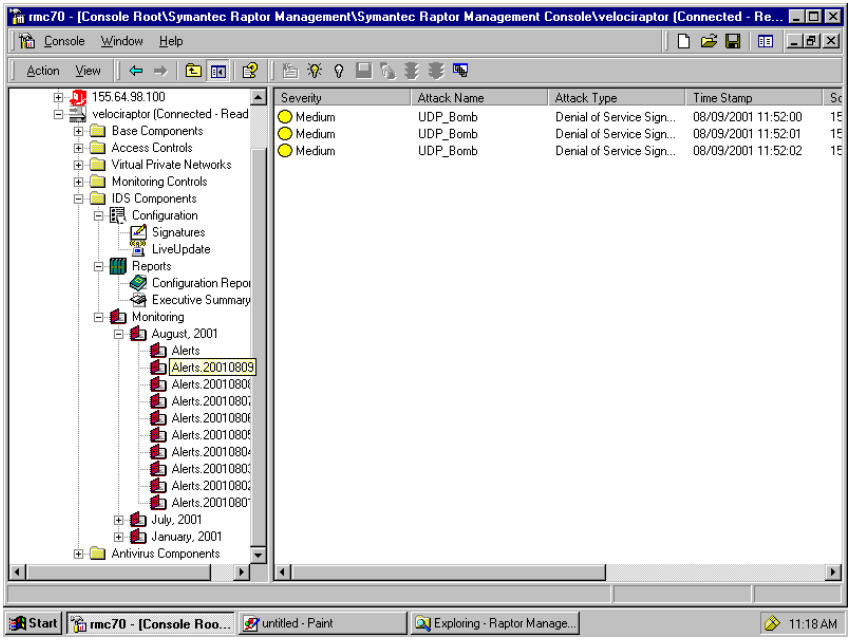


Figure 8-3 IDS Alerts Viewer page

When an IDS attack is detected, an entry is made in the file named `logfile.YYYYMMDD`, where `YYYYMMDD` represents the year, month, and day the log was created. These attacks appear in the IDS Alerts Viewer when you access that file via the IDS Monitoring node.

New log messages appear at the bottom of the window, scrolling up previous log messages. The SRMC automatically updates the view of the current logfile every 15 seconds while the IDS Alerts Viewer is open.

Logfiles are managed using a program called changelog. For more information, see **Manage log files on page 127**.

You can view additional information about each entry in the IDS Alerts Viewer by double clicking on an event.

For more information, see **Viewing additional information for a signature on page 139**.

To view IDS events in the Alerts Viewer

1. In the left pane, expand the **IDS Components** branch, and then expand the **Monitoring** branch.
2. Expand the folder that contains the alerts that you want to view.
3. Click the alerts icon for the file that you want to view.

   The most current events in the selected log appear in the right pane. An entry appears for each IDS logfile entry. The information includes:

   Severity: The assigned severity of the attack; levels are High, Medium, and Low.

   Attack Name: The name of the attack signature.

   Attack Type: The type of attack.

   Timestamp: The time the attack was logged on the appliance.

   Source IP: The source IP address of the attack.

   Destination IP: The destination IP address of the attack.

   OS Impacted: The operating systems that can be affected by this attack.
4. Click on an alert in the right pane, then click **Page Up** on the keyboard to view the previous alerts logfile.

   Click **Page Up**, **Page Down**, **Home**, and **End** on the keyboard to navigate to all records in the IDS Alerts Viewer.

Updating the View in the IDS Alerts Viewer

Though the SRMC automatically updates the view of the current logfile every 15 seconds while the IDS Alerts Viewer is open, you can update the view of the logfile at any time.

To update the view of the current logfile

- Right click in either the left or the right pane, and then press F5.

IDS Reports

You can generate both an Executive Summary report and a Configuration report that contain IDS information for an appliance.

Configuration Report

The Configuration Report provides the current configuration of each attack signature, along with configuration information for LiveUpdate for the selected appliance.

To generate a Configuration report

1. Select the appliance for which you want to generate a report.
2. Expand the **IDS Components** branch.
3. Expand the **IDS Reports** branch, and then click **Configuration Report**.

   The report, ConfigReport.htm, appears in the right pane and is saved to:

   ```
   Program Files\Symantec\Raptor Management Console\
       reports\IDS\appliance IP\
   ```

   where *appliance IP* is the IP address of the appliance.

Executive Summary

The Executive Summary report is a high-level overview of the number and risk level of attacks seen during a specified date range, including a list of all alerts, categorized by High, Medium, or Low, in reverse chronological order. For each alert, the alert name, the source IP, and destination IP are read from the logfiles, and then the severity and attack type are read from the signature configuration file.

A fourth category of Other may appear in the report. Alerts would fall into this category if they appear in the logfile and the signature that triggered them has been removed from the current signature configuration file on the appliance.

Executive Summary reports are a good way to take periodic snapshots of your overall network security.

Generating a new Executive Summary report

To generate an Executive Summary report

1. Select the appliance for which you want to generate a report.

2 Expand the **IDS Components** branch.

3 Expand the **IDS Reports** branch, and then click **Executive Summary**.

4 Right click in the right pane, and then click **Run New Report**.

5 In the New Executive Summary Report dialog box, specify the date/time range for the report.

6 Click **OK**.

The Creating Report dialog box appears, indicating report generation progress, then the report data appears in a new browser window.

7 After viewing the report, close the browser window to return to the SRMC.

Each report is saved to:

`Program Files\Symantec\Raptor Management Console\ reports\IDS\`*`appliance IP`*`\`*`ExecSumYYYYMMDDHHMMSS`*`.htm`

where *appliance IP* is the IP address of the appliance and where *YYYYMMDDHHMMSS* is the year, month, day, hour, minute and second that the report was generated.

Viewing an existing Executive Summary report

To view an existing Executive Summary report

1 Select the appliance for which you want to view a report.

2 Expand the **IDS Components** branch.

3 Expand the **IDS Reports** branch, and then click **Executive Summary**.

4 In the right pane, double click the report that you want to view.

The report data appears in a new window.

Deleting an existing Executive Summary report

To delete an existing Executive Summary report

1 Select the appliance for which you want to view a report.

2 Expand the **IDS Components** branch.

3 Expand the **IDS Reports** branch, and then click **Executive Summary**.

4 In the right pane, click the report that you want to delete.

5 Right click, then click **Delete Report**.

6 In the confirmation dialog box, click **Yes**.

IDS notifications

Notifications provide a way to alert designated individuals or systems when messages are logged on your appliance.

This section describes the notifications you can send in response to IDS Alerts.

You can specify the type of notification the appliance sends, and the level of severity that will trigger the notification.

Note: IDS alerts constitute message numbers 525, 550, and 575. If system notifications are configured to notify on Warning-level events (500 series events), IDS alerts will not trigger the system notification. You must create IDS notifications to trigger notifications by severity level for IDS alerts.

To configure any kind of IDS notification

1. Expand the **Monitoring Controls** folder and select the **Notifications** icon.
2. Right click and choose **New>IDS Notification** to create a notification that will apply only to messages sent by the Intrusion Detection System (IDS).

The General tab of the Notifications Properties page is displayed, with IDS only shown in the **Type** field.

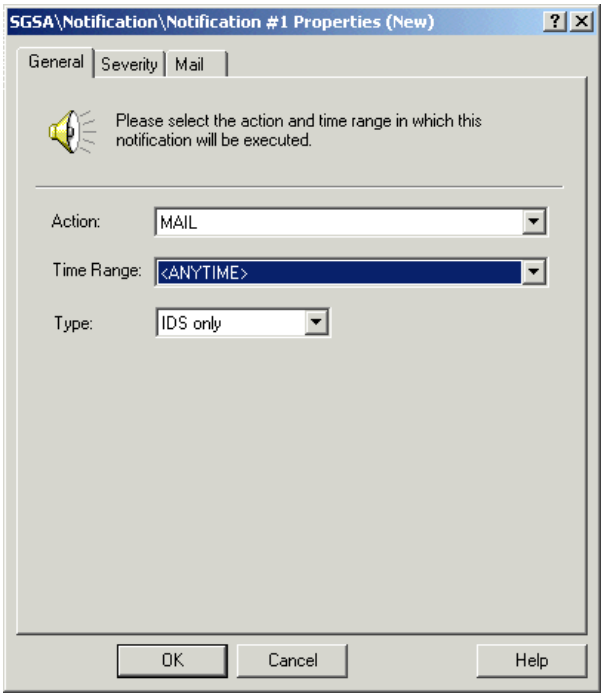


Figure 8-4 Notifications Properties Page – General Tab

You can use the Type list to change the type of notification to a System notification.

Changing the type changes the choices available from the Action drop-down list and the options available on the Severity tab.

For instructions on creating system notifications, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

3 Use the **Action** drop-down list to choose the way in which the notification will take place.

BLACKLIST: Sends the blacklist notification to a specified firewall address

CLIENT PROGRAM: Launches a client program

MAIL: E-mails the text of the log message to a designated person

PAGE: Transmits a message to a designated paging device

SNMPV1: Sends an SNMP alert to a designated system

SNMPV2: Sends an SNMP alert to a designated system

Depending on the action you select, an additional tab will be displayed.

4 Use the **Time Range** drop-down list to select the time range during which this notification applies.

Use <ANYTIME> if you want the notification to be active at all times.

Access the Time Range Properties page to create a new Time Range. Once created, the Time Range is selectable via the drop-down list. For more information about setting Time Ranges, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

5 Use the tab that was displayed when you selected an action to configure details of the notification.

The following sections describe the configuration of the different kinds of notifications.

6 Click the **Severity** tab.

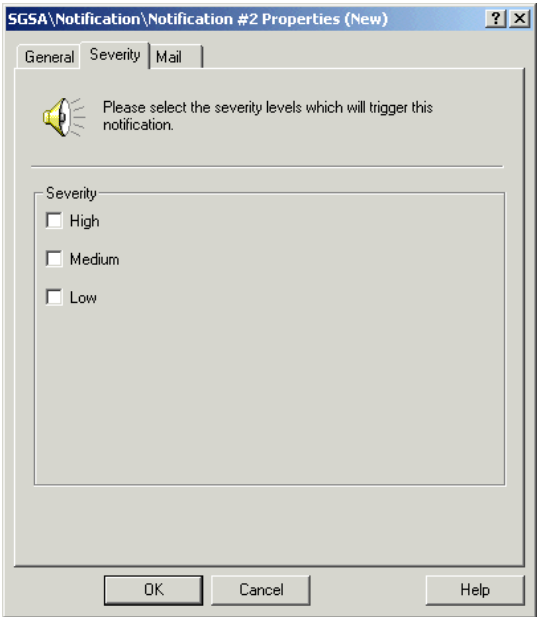


Figure 8-5 Notifications Properties Page – Severity Tab

IDS messages are classified as High, Medium, and Low.

7 Select one or more of the check boxes to choose the severity level or levels for which the notification will be triggered.

8 Click **OK** to save your Notification.

Blacklist notifications

When you configure one or more Blacklist notifications, the Notify daemon looks for IDS Alert messages and sends messages to the blacklist daemon on the specified firewall.

The firewall then blocks traffic from the source IP address (specified in the IDS Alert message) for the blacklist time specified.

Note: Blacklist notifications are only available with an appliance that has Intrusion Detection System (IDS) enabled.

To configure a Blacklist notification

1. Expand the **Monitoring Controls** folder and select the **Notifications** icon.
2. Right click and choose **New>IDS Notifications** to display the General tab of the Notification Properties page.
3. Choose **BLACKLIST** from the Action drop-down list.
4. Click the **Severity** tab.
5. Check one or more of the check boxes to choose the severity level or levels for which the notification will be triggered.

6 Click the **Blacklist** tab.

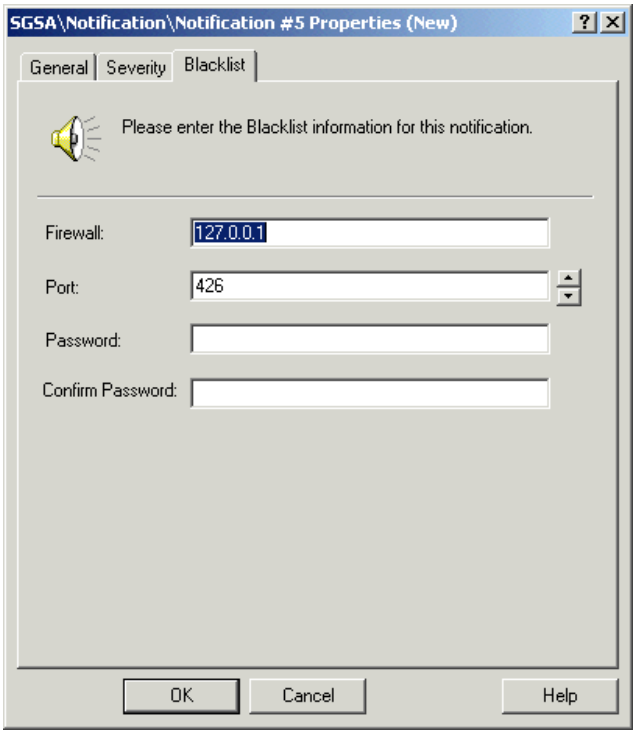


Figure 8-6 Notifications – Blacklist Tab

7 In the **Firewall** field, enter the IP address of the firewall to which the Blacklist notification will be sent.

The default is the appliance where IDS is running (127.0.0.1).

8 In the **Port** field, enter the firewall's Blacklistd port number or accept the default port 426.

9 In the **Password** field, enter the password that Blacklist will use to authenticate itself with the firewall.

Record this password so that you can use it when you create the remote management password for the blacklist daemon, as shown in the next procedure.

10 Re-enter the password to confirm it.

11 Click **OK**.

After you create the notification, you must configure the blacklist daemon on the system that will receive the notification.

To configure the blacklist daemon

1. Connect to the firewall that will receive the notification.
2. Expand the **Base Components** node.
3. Right click on **Remote Management Passwords** and choose **New** > **Remote Management Password**.
4. In the Remote Management Password Properties page, click the **Intrusion Detection** radio button.
5. Leave the port number for intrusion detection at 426.
6. Use the **Blacklist Timeout** field to specify the duration of the blacklist period.

   By default, this field is set to 1440 minutes, which equals 24 hours.
7. Enter the IP address of the system that will be sending the notification.
8. Enter the password of the system that will be sending the notification.
9. Re-enter the password to verify it.
10. Click OK.

Client Program notification

A Client Program notification causes the appliance to start up a designated client program in response to an IDS alert.

To configure a Client Program notification

1. Expand the **Monitoring Controls** folder and select the **Notifications** icon.
2. Right click and choose **New>IDS Notifications** to display the General tab of the Notification Properties page.
3. Choose **CLIENT PROGRAM** from the Action drop-down list.
4. Click the **Severity** tab.
5. Check one or more of the check boxes to choose the severity level or levels for which the notification will be triggered.

Click the **Client Program** tab.

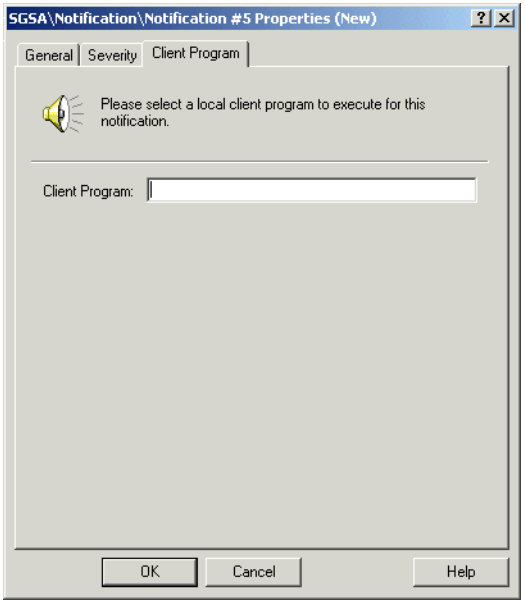


Figure 8-7 Notifications – Client Program Tab

6 In the **Client Program** field, enter the full path of the client program you want to invoke plus any arguments.

The appliance will call the program as it appears in the Name field, appending the date and contents of the message text to the end.

Note: Any client program you call MUST exit upon completion. Multiple copies of your program can run at once.

---

7 Click **OK** to save your notification.

Mail notifications

A Mail notification sends the text of a message to the person you designate.

Note: Mail notification messages are NOT encrypted. The text of the message is clear text. Information on the operation of your appliance included in Mail Notifications could be used in an attack. For this reason, plan your notifications carefully so that they will not go over public networks.

To configure a Mail notification

1. Expand the **Monitoring Controls** folder and select the **Notifications** icon.
2. Right click and choose **New>IDS Notifications** to display the General tab of the Notification Properties page.
3. Choose **MAIL** from the Action drop-down list.
4. Click the **Severity** tab.
5. Check one or more of the check boxes to choose the severity level or levels for which the notification will be triggered.
6. Click the **Mail** tab.

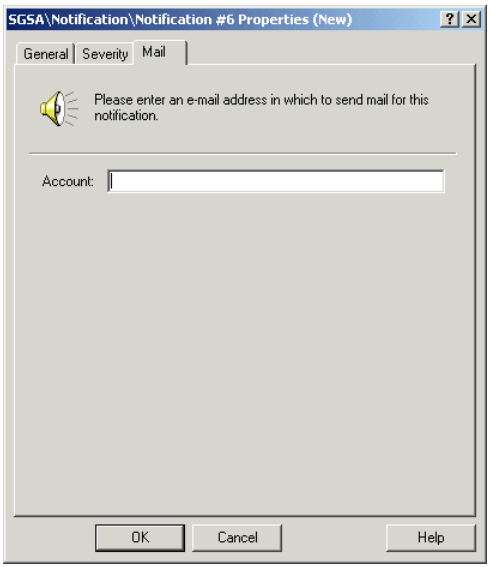


Figure 8-8 Notifications – Mail Tab

7. In the Account field, enter the e-mail address of the mail recipient.

   The hostname portion of the e-mail address must be the hostname of the mail server and the recipient must have an account or alias on that server.

   The notification program does not understand MX records, only addresses.

   When you specify a mail address in the form jane@acme.com, the appliance must be able to convert acme.com directly into an IP address. You can accomplish this by making an entry for acme.com in the appliance's hosts file. For more information, see **Provide private DNS file address statements on page 104**.
8. Click **OK** to save your notification.

Page notifications

A Page notification causes the appliance to page a recipient.

Note: To use page notifications, you must have a Hayes-compatible modem and you must specify its COM port through the NOTIFYD Properties page.

To configure a Page notification

1. Expand the **Monitoring Controls** folder and select the **Notifications** icon.
2. Right click and choose **New>IDS Notifications** to display the General tab of the Notification Properties page.
3. Choose **PAGE** from the Action drop-down list.
4. Click the **Severity** tab.
5. Check one or more of the check boxes to choose the severity level or levels for which the notification will be triggered.
6. Click the **Page** tab.

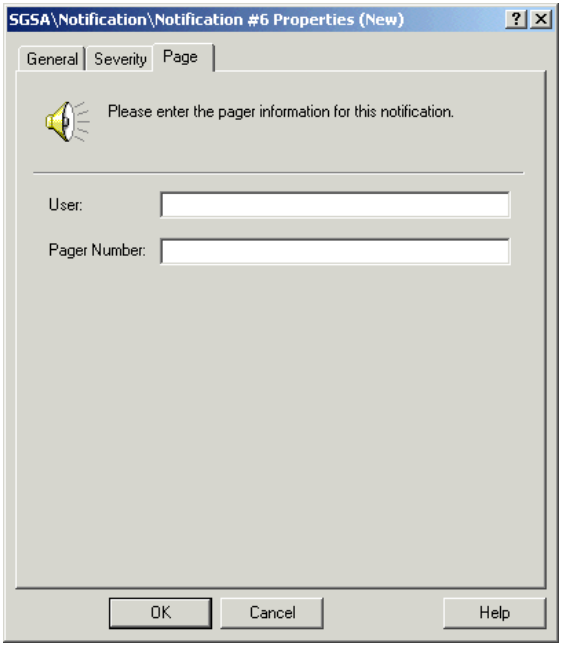


Figure 8-9 Notifications – Page Tab

7 Complete one of the following procedures.

To specify a numeric Page notification

a Enter the user name of the page recipient in the **User** field.

For numeric pagers, the name field is an identifier within SRMC.

b Enter the recipient's phone number and PIN in the **Pager Number** field, using commas to indicate pauses in the dialing sequence. Paging tends to be sensitive to timing. You will need to experiment by adding or removing commas.

Complete the sequence with a numeric code followed by "#;"(pound sign and semicolon only.)

For example, if a recipient is using a numeric pager with a phone number of 111-2222, a PIN of 1234, and a numeric code of 9999, the entry in the Phone field would be as follows:

1112222,,,,,1234,,,,9999#;

The pager displays the numeric code when activated.

To specify an alphanumeric Page notification

a Enter the PIN of the page recipient in the **User** field.

b Enter the recipient's phone number in the **Page Number** field, using commas to indicate pauses in the dialing sequence.

For example, if a recipient is using an alphanumeric pager with a phone number of 111-2222 and a PIN of 1234, the entries in the user and page number fields would be as follows:

1234

1112222

The pager displays the text of the log message when activated.

Note: The paging provider must support the TAP protocol (also known as the Motorola/IXO alphanumeric paging protocol). Set your modem speed to 2400 or even 300 bps to maintain compatibility with the TAP protocol definition.

---

8 Click **OK** to save your page notification.

You must also specify the com port that will be used to connect to the pager.

To specify the com port

1 Expand the **Base Components** folder.

2 Click the **Gateway Services** icon and then double click **NOTIFYD** in the right pane.

3 Select the **Com Port** tab and choose the appropriate com port from the pull-down menu.

Comport 0 is the default for paging.

4 Click **OK**.

SNMP notifications

You can configure the Symantec Gateway Security appliance to send traps containing alert messages to network management stations. Currently, two versions of SNMP exist:

- SNMPv1
- SNMPv2

The SRMC Notifications Properties page enables you to specify each type of SNMP notification. The firewall does not support gets and sets by SNMP.

You follow the same process in setting up SNMPv1 and SNMPv2 notifications as for other notification types. The only difference consists in the information you must enter in SRMC's text fields. This information must be supplied by the system administrator of the device to which the appliance sends SNMP traps.

For SNMP managers to understand traps, the names of any device-specific variables to be exchanged must be agreed upon. Their variable names are stored in the Management Information Base (MIB) of the agent and manager software. Although the appropriate MIB values for Symantec Gateway Security appliance SNMP alerts are pre-configured in the appliance, SNMP management stations that receive alerts from the appliance must have this information incorporated into their MIBs.

To support this configuration task, the Symantec Gateway Security appliance distribution CD includes MIB files for SNMPv1 and SNMPv2 alerts. Their locations are:

Table 8-1 SNMP Notification MIB Files

Filename	Location
snmpv1.mib	Symantec Gateway Security CD\ClientSoftware\snmp\
snmpv2.mib	Symantec Gateway Security CD\ClientSoftware\snmp\

Configuring an SNMPV1 notification

Before you begin to create a notification, contact the system administrator of the SNMP device to which you want to send the notification to get the host name and port number of the SNMP device, and a value for the Community field.

To configure an SNMP V1 notification

1. Expand the **Monitoring Controls** folder and select the **Notifications** icon.
2. Right click and choose **New>IDS Notifications** to display the General tab of the Notification Properties page.
3. Choose **SNMP V1** from the Action drop-down list.
4. Click the **Severity** tab.
5. Check one or more of the check boxes to choose the severity level or levels for which the notification will be triggered.
6. Click the **SNMP V1** tab.

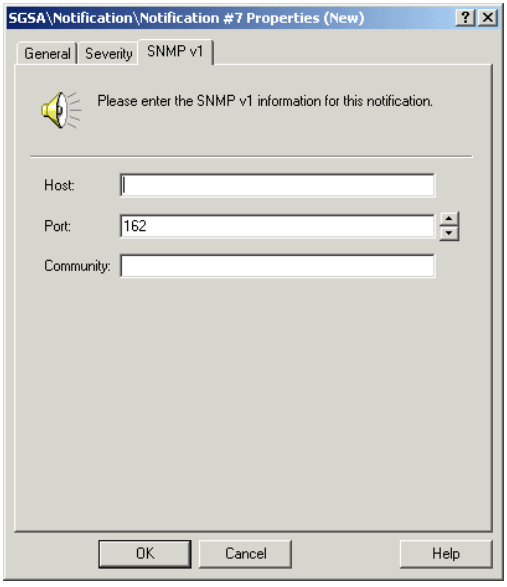


Figure 8-10 Notifications – SNMP V1 Tab

7. Enter the **Host** name and **Port** number supplied by the SNMP system administrator.
8. In the **Community** field, enter the text string provided by the system administrator of the SNMP device to which you want to send the notification. The optional default value is public.

9 Click **OK** to save your notification.

Configuring an SNMPV2 notification

Before you begin to create the notification, contact the system administrator of the device to which the firewall sends SNMP traps for the host name and port number and the OID values for the source and destination parties and the trap context.

To configure an SNMP V2 notification

1 Expand the **Monitoring Controls** folder and select the **Notifications** icon.

2 Right click and choose **New>IDS Notifications** to display the General tab of the Notification Properties page.

3 Choose **SNMP V2** from the Action drop-down list.

4 Click the **Severity** tab.

5 Check one or more of the check boxes to choose the severity level or levels for which the notification will be triggered.

6 Click the **SNMP V2** tab.

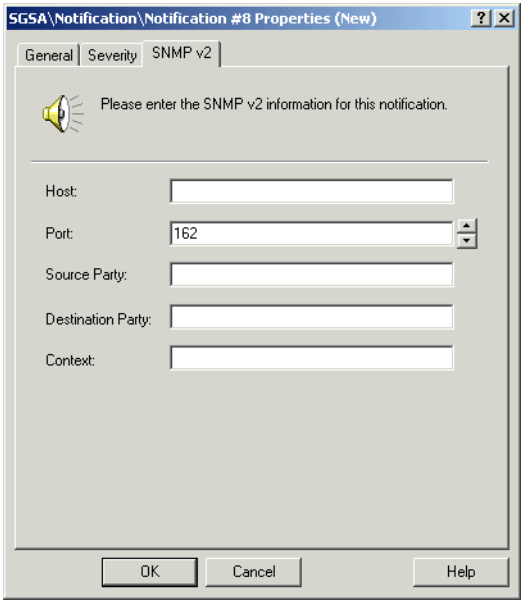


Figure 8-11 Notifications – SNMP V2 Tab

This tab provides the information necessary to support unauthenticated, non-private traps.

7 Enter the **Host** name and **Port** number provided by the SNMP system administrator.

8 Complete the **Source Party**, **Destination Party**, and **Context** fields by entering the OID values provided by SNMP administrator.

An OID is a sequence of integers separated by periods, such as 1.3.1.6.1.4.

9 Click **OK** to save your notification.

Chapter 9

Antivirus Scanning

The possibility of a virus attack is a serious negative aspect of the Internet. Viruses can easily spread in the Internet environment and pose major threats to critical business operations and financial investment. Implementing antivirus protection at the firewall is a critical step in protecting your network against viruses and other related threats. The Symantec Gateway Security appliance provides comprehensive virus protection and lets you control antivirus scanning by individual proxy so you can configure virus protection specifically to meet your needs.

Antivirus scanning on the Symantec Gateway Security appliance is implemented as a client/server relationship. The SMTP, HTTP, and FTP proxies on the appliance are configured to act as clients that pass files to the antivirus scan server. When you specify antivirus scanning for a particular proxy, files are passed by the proxy to the antivirus scan server, which in turn scans the files for viruses and mail policy violations. Files that have unrepairable infections or that violate the established mail policy are blocked, while clean files and infected files that can be repaired are allowed to pass through.

About Symantec AntiVirus

Symantec Gateway Security features Symantec AntiVirus technology via an antivirus scan server installed on the appliance. The Symantec Gateway Security antivirus scan server detects viruses, worms, and Trojan horses in all major file types (for example, Windows files, DOS files, and Microsoft Word and Excel files). The antivirus scan server also detects mobile code, such as Java™, ActiveX®, and standalone script-based threats. Symantec Gateway Security utilizes Symantec's key antivirus engine technologies, including Bloodhound™ for heuristic detection of new or unknown viruses and Symantec's Norton AntiVirus Extension (NAVEX)™, which provides protection from new classes of viruses automatically via LiveUpdate.

The Symantec Gateway Security appliance antivirus scan server also includes a decomposer that handles compressed file formats and nested levels of files. For embedded files, scanning can be limited to certain file types based on extension.

The scan server handles the following archival and encoded file types:

- .amg
- .arj
- .gzip
- mime
- .lha
- .tar
- .uue
- .zip

Symantec AntiVirus technology is fully supported by the Symantec Security Response Team™. Symantec's Security Response engineers work 24 hours per day, 7 days per week, tracking new virus outbreaks and identifying new virus threats.

Virus detection

When Symantec engineers identify a new virus, information about the virus (a virus signature) is stored in a virus definitions file. Virus definitions files are updated periodically via Symantec's automated LiveUpdate feature. When the Symantec Gateway Security antivirus scan server scans for viruses, it is searching for these virus signatures. To supplement detection of virus infections by virus signature, the antivirus scan server includes Symantec's patented Bloodhound technology, which heuristically detects new or unknown viruses, based on the general characteristics exhibited by known viruses.

Bloodhound heuristic technology

Researchers at Symantec have developed two types of heuristics for Symantec AntiVirus. The first, Bloodhound, is capable of detecting upwards of 80 percent of new and unknown executable file viruses. The second, Bloodhound-Macro, detects and repairs over 90 percent of new and unknown macro viruses. These statistics are staggering considering the growth rate of computer viruses. Bloodhound requires minimal overhead since it examines only programs and documents that meet stringent prerequisites. In most cases Bloodhound can determine in microseconds whether a file or document is likely to be infected by a virus. If it determines that a file is not able to be infected, it immediately goes on to the next file.

Bloodhound and executable viruses

Bloodhound uses artificial intelligence (AI) technology to isolate and locate the various logical regions of each program it is told to scan. It analyzes the program logic in each of these components for virus-like behavior and simulates this behavior to determine whether the program is a virus.

Bloodhound and macro viruses

Symantec Bloodhound-Macro technology uses a hybrid heuristic scheme to detect and repair more than 90 percent of all new and unknown macro viruses automatically. For example, every time the antivirus scan server scans a Microsoft Word document, Bloodhound-Macro sets up a complete virtual Word environment into which it loads the document. The macros contained in the document are run as they would be in the word processing application. Bloodhound-Macro monitors the macros as they run and watches for them to copy themselves from the host document to another virtual document. Bloodhound-Macro also stimulates the copied macros and verifies that they can further propagate.

Norton AntiVirus Extension (NAVEX)™ technology

NAVEX is a technology that lets Symantec update the scanning engine during routine virus definitions updates. That means no inline revisions or time-consuming upgrades are necessary to ensure that your antivirus protection stays current, regardless of platform, even against new virus threats.

The scanning engine is made up of dozens of complex search algorithms, CPU emulators, and other program logic. The scanning engine examines a file to determine whether the file contains viruses. The scanning engine scans files and disks for virus fingerprints (unique sequences of bytes known to be contained in viruses). These fingerprints are stored in the virus definitions files downloaded each week. The scanning engine also repairs infected files.

Occasionally, a new virus or class of viruses emerges that cannot be detected by existing scanning engines. These viruses require new algorithms for detection—and consequently a new scanning engine. With the NAVEX technology, Symantec engineers can quickly upgrade the fundamental Symantec AntiVirus scanning engines, with no extra cost or effort required on the part of the customer.

Striker technology

Striker technology identifies polymorphic computer viruses, which are the most complex and difficult viruses to detect. Like an encrypted virus, a polymorphic virus includes a scrambled virus body and a decryption routine that first gains control of the computer, and then decrypts the virus body. However, a polymorphic virus also adds a mutation engine that generates randomized decryption routines that change each time a virus infects a new program. As a result, no two polymorphic viruses are the same.

Each time Striker scans a new program file, it loads the file into a self-contained virtual computer. The program executes in this virtual computer as if it were running on a real computer. Inside this virtual computer, the polymorphic virus runs and decrypts itself. Striker then scans, detects, and repairs the virus.

LiveUpdate™

Symantec's LiveUpdate™ technology ensures that you are not at risk of infection by newly discovered viruses. Updated virus definitions files, which contain the necessary information to detect and eliminate viruses, are supplied by Symantec at least every week and whenever a new virus threat is discovered. The Symantec Gateway Security appliance can be configured to poll the Symantec LiveUpdate servers to determine whether updated definition files have been posted. If new

virus definitions are available, Symantec Gateway Security downloads the proper files and installs them in the proper location. Virus protection stays current without interruption in protection.

Antivirus scanning on the Symantec Gateway Security appliance

The Symantec Gateway Security antivirus scan server listens on a TCP/IP address and port number. The SMTP, HTTP, and FTP proxies on the Symantec Gateway Security appliance are configured to act as clients that pass files for scanning to the antivirus scan server via this port.

The Symantec Gateway Security appliance can be configured to do any of the following through the antivirus scan server:

- Perform antivirus scanning

  Also, depending on your configuration, the antivirus scan server can attempt repair of infected files and delete those files that cannot be repaired.
- Enforce a configurable mail policy, where the scan server scans mail messages for policy violations based on the mail policy you establish for incoming and outgoing SMTP traffic

  Note: Some of these mail filters can be used during an e-mail-born virus outbreak to further protect your network. For example, once you have information on the characteristics of a new virus, you can use this information to block an infected mail message right at the firewall, before it affects your network. You can protect your network immediately, even before virus definitions for the new virus have been posted.
- Add a customizable message to mail messages where an infected attachment has been repaired
- Add a customizable message to mail messages where an infected attachment has been deleted because it could not be repaired

Configuring antivirus scanning

To implement antivirus scanning on the Symantec Gateway Security appliance, you must do the following:

- Configure the antivirus scan server via the Antivirus Components node, including:

  - Specifying the bind address and port number on which the antivirus scan server listens

    For more information, see **Configuring the antivirus scan server on page 168**.
  - Configuring LiveUpdate to ensure that your virus protection remains current

    For more information, see **Updating virus definitions on page 171**.
  - Establishing your mail filter policy to optionally block mail based on total message size, attachment size or file name, message subject, or message origin

    For more information, see **Using the mail filter options on page 186**.

- Create specific rules, via the Rules icon under the Access Controls node, to implement antivirus scanning by specifying FTP, HTTP, or SMTP as a service and enabling antivirus scanning for that service or create a rule that allows multiple services which can each have antivirus enabled

  For more information, see **Enabling antivirus scanning in a rule on page 183**.
- Configure the way in which antivirus scanning is implemented for each proxy service (FTPD, HTTPD, and SMTPD) via the Antivirus Scanning tab on the Proxy Services properties page for each proxy

  For more information, see **Configuring proxy services for antivirus scanning on page 173**.

When you create specific rules for SMTP, HTTP, or FTP, you must enable antivirus scanning for any rule for which antivirus scanning is to occur. You can have multiple rules for a given proxy, and antivirus scanning must be enabled independently for each rule. For each proxy service (SMTPD, HTTPD, and FTPD), you configure the manner in which antivirus is implemented for that proxy. For example, the Proxy Services configuration you set up for FTPD determines how virus scanning is implemented for all rules for which FTP is enabled as a service and for which antivirus scanning is enabled.

Local versus remote scanning

For most networks, all virus scanning will be local. That is, virus scanning for all proxies is handled by the single antivirus scan server on the same appliance as the proxies themselves. If you are using multiple Symantec Gateway Security appliances or clusters, you may want to allow remote (serviced by an antivirus scan server on another Symantec Gateway Security appliance) antivirus scanning for one or more proxies. The independent configuration options for each proxy

service (SMTPD, HTTPD, and FTPD) let you point to another antivirus scan server on another appliance for scanning on one or more proxies.

The Global_Antivirus_Configuration Properties page lets you configure the local antivirus scan server. The IP address and port number that you select for the local scan server can be used to control whether remote scanning for another appliance is permitted. If permitted, the local antivirus scan server will service connections from proxies on other appliances.

For more information, see **Configuring the antivirus scan server on page 168**.

The Proxy Services configuration for each individual proxy lets you select the IP address and port number of the antivirus scan server that will handle the antivirus scanning for that proxy. If scanning is to be provided by a scan server on another appliance, use the IP address for that appliance and the port number on which the scan server on that appliance is listening. If scanning will be local (performed by the antivirus scan server on the same appliance as the proxy), the configuration for that proxy should point to the local antivirus scan server.

For more information, see **Configuring proxy services for antivirus scanning on page 173**.

Configuring the antivirus scan server

The antivirus scan server is configured via the Antivirus Components node. Under the Configuration icon, the Global_Antivirus_Configuration Properties page lets you specify the bind address and port number on which the antivirus scan server listens. Proxies pass files to be scanned to the antivirus scan server via this port. The port number must be exclusive to the antivirus scan server. The default port number is 1344.

The bind address you select can depend on how you plan to distribute the workload for Symantec Gateway Security antivirus scanning on your network. You can limit the scan server to local scanning only or allow remote connections to the antivirus scan server.

The bind address and port number specified in the proxy configuration for any proxy (FTPD, HTTPD, or SMTPD) that will pass files for scanning to the antivirus scan server must correspond to the bind address and port number selected here.

For more information, see **Configuring proxy services for antivirus scanning on page 173**.

To configure the antivirus scan server

1. In the left pane, expand the **Antivirus Components** node.
2. Click **Configuration**.

3 Double click **Global_Antivirus_Configuration** in the right pane to display the Global_Antivirus_Configuration Properties page.

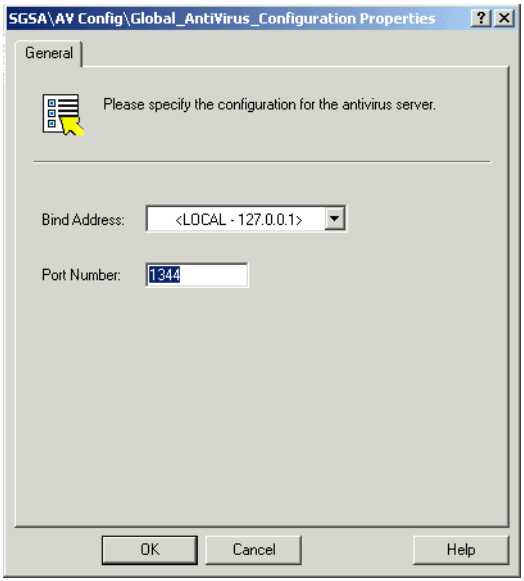


Figure 9-1 AV Global Antivirus Configuration Properties Page – General Tab

4 Use the **Bind Address** drop-down list to specify the IP address on which the local antivirus scan server listens.

Your choices are:

<LOCAL 127.0.0.1>

This address is known as the loopback interface. In this configuration, the antivirus scan server only accepts connections from proxies that are running on the same appliance. If you select the loopback interface, you must use the same setting for any proxy (under the Proxy Services configuration for that proxy) for which scanning will be local.

<ALL – 0.0.0.0>

If you select ALL, the antivirus scan server accepts all requests that it receives (local and nonlocal).

eth0

If you select eth0, the antivirus scan server accepts only scan requests from the eth0 interface. By default, this is the inside interface.

eth1

If you select eth1, the antivirus scan server accepts only scan requests from the eth1 interface. By default, this is the outside interface.

Note: On some appliances, additional interfaces may be available.

---

5 Enter the TCP/IP **Port Number** on which the antivirus scan server listens.

This port number must be exclusive to the antivirus scan server. The default port number is 1344. If you use a port number other than the default, select a number greater than 1024 that is not in use by any other program or service.

6 Click **OK** to save your configuration.

Updating virus definitions

The virus definitions used by the Symantec Gateway Security appliance to detect and repair viruses are updated using Symantec's LiveUpdate technology. Updated virus definitions files are supplied by Symantec at least every week and whenever a new virus threat is discovered. The Symantec Gateway Security appliance can be configured to poll the Symantec LiveUpdate servers periodically to check for updated definition files. If new virus definitions are available, the proper files are downloaded and installed in the proper location.

Note: You must have an Internet connection in order to run LiveUpdate.

For each appliance connected to the SRMC, you can:

- Run LiveUpdate on demand
- Schedule LiveUpdate to run at a specific time

If you are using a cluster or multiple Symantec Gateway Security appliances, each appliance must be updated separately.

Note: Virus definitions are not configurable. Virus definitions are only updated when LiveUpdate is run.

Caution: If you do a factory reset of your appliance, you will loose the most recent virus definitions and all LiveUpdate schedule information. You will have only the virus definitions that were running on the appliance when it was first installed and you will need to re-schedule LiveUpdate.

Following a factory reset, run LiveUpdate immediately to update the virus definitions. Symantec recommends that you schedule regular LiveUpdates to ensure that you are protected against new virus threats.

Running LiveUpdate on demand

You can run LiveUpdate at any time to update the virus definitions for the antivirus scan server.

To run LiveUpdate on demand

1 In the left pane, expand the **Antivirus Components** node.

2 Click **LiveUpdate**.

The right pane displays LiveUpdate status information, including the date and version number of the last successful update.

3 Double click the status information to display the AV LiveUpdate Properties page.

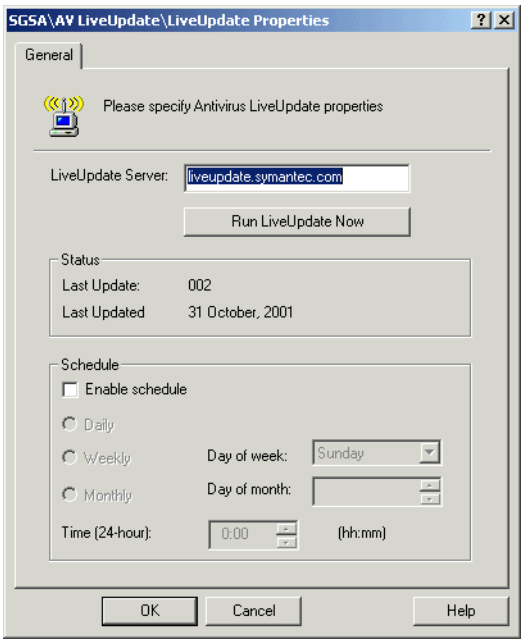


Figure 9-2 AV LiveUpdate Properties Page

4 Verify that the **LiveUpdate Server** field contains the domain name of the correct LiveUpdate server; change the name if necessary.

The default setting is liveupdate.symantec.com. In most cases, you will not need to edit this setting.

Note: If you change the server address, you must save this information before you proceed with step 5. After changing the server address, click **OK** to close the AV LiveUpdate Properties page, then click **Save and Reconfigure** on the toolbar. Open the property page again, and then proceed with step 5.

---

5 Click **Run LiveUpdate Now**.

A message notifies you that LiveUpdate has been run successfully. A logfile is also created to show the update.

6 Click **OK** to close the AV LiveUpdate Properties page.

Scheduling LiveUpdate to run automatically

You can schedule LiveUpdate to run on an appliance at the same time every day, the same time on a specific day every week, or at the same time on the same day of every month.

To schedule LiveUpdate to run automatically

1 In the left pane, expand the **Antivirus Components** node.

2 Click **LiveUpdate**.

The right pane displays LiveUpdate status information, including the date and version number of the last successful update.

3 Double click the status information to display the LiveUpdate Properties page.

4 Verify that the **LiveUpdate Server** field contains the domain name of the correct LiveUpdate server; change the name if necessary.

The default setting is liveupdate.symantec.com. In most cases, you will not need to edit this setting.

5 Check **Enable Schedule**.

6 Do one of the following:

- Click **Daily** to run LiveUpdate every day. Select the **Time** to run LiveUpdate.
- Click **Weekly** to run LiveUpdate at the same time on the same day of every week. Select the **Day of week**, and select the **Time** to run LiveUpdate.
- Click **Monthly** to run LiveUpdate at the same time on the same day of every month. Select the **Day of month**, and select the **Time** to run LiveUpdate.

7 Click **OK**.

LiveUpdate runs automatically as scheduled.

Configuring proxy services for antivirus scanning

The client component of the antivirus implementation is configured through the HTTPD, FTPD, and SMTPD Proxy Services configuration. In the configuration for each proxy service, you configure the way in which antivirus is implemented for that proxy. When you create specific rules for a given proxy and enable

antivirus scanning for those rules, the antivirus settings you configure via the Proxy Services configuration apply to the antivirus scanning for that proxy.

The proxy configuration for each proxy lets you specify the following:

- the address and port number of the scan server that will provide scanning services
- the handling of files when the antivirus scan server is unavailable
- the handling of infected files; and the types of files (by extension) that will be submitted to the antivirus scan server for scanning

The proxies do not have to be running on the same physical appliance as the antivirus scan server. The functionality is identical regardless of whether the antivirus scan server is local or remote to the proxies. The proxy establishes a TCP/IP connection to the antivirus scan server and passes the file to be scanned to the scan server. The scan server scans the file and handles it based on the configuration settings established for that proxy.

Configuring antivirus scanning for the FTP and HTTP proxies

The Proxy Services configuration you set up for FTPD or HTTPD, respectively, determines how virus scanning is implemented for all rules for which FTP or HTTP is enabled as a service and for which antivirus scanning is enabled.

To configure the antivirus settings for FTP or HTTP

1. In the left pane, expand the **Access Controls** node.
2. Click **Proxy Services**.
3. In the right pane, double click **FTPD** to display the FTPD Proxy Properties page or **HTTPD** to display the HTTPD Proxy Properties page.
4. Click the **Antivirus Scanning** tab.

Use this tab to control the behavior of virus scanning.

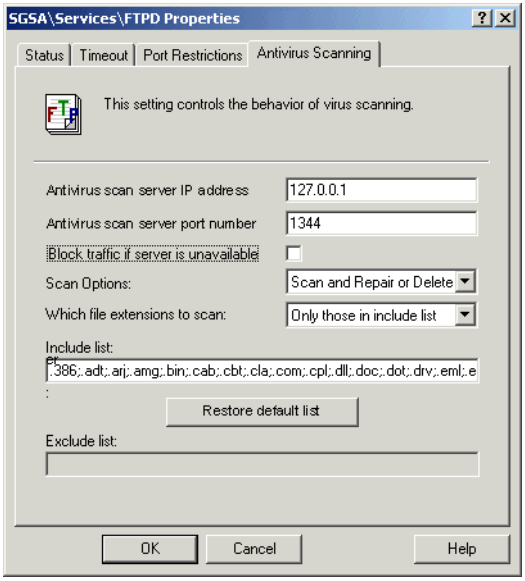


Figure 9-3 FTPD Properties – Antivirus Scanning Tab

5 In the **Antivirus scan server IP address** field, enter the IP address of the antivirus scan server that will be used to scan for viruses.

The bind address you select here is dependent on whether you want local or remote scanning and on how the antivirus scan server that will do the scanning has been configured. Use the following table for guidance.

Table 9-1 Configure the antivirus settings for FTP or HTTP

Configuration	Bind address selected under antivirus scan server global config	Scan server IP address selected here for proxy configuration
The antivirus scan server and the proxy are on the same appliance, and the scan server is configured to accept only local connections	127.0.0.1 (the loopback interface)	127.0.0.1 (the loopback interface)
The antivirus scan server and the proxy are on the same appliance, and the scan server is configured to accept both local and remote connections	0.0.0.0, eth1, or eth0	The physical IP address of the appliance running both the proxy and the antivirus scan server
The proxy will request scanning from an antivirus scan server on a different appliance (thus, that scan server is configured to accept remote connections from this appliance)	0.0.0.0, eth1, or eth0	The physical IP address of the appliance running the antivirus scan server

6 In the **Antivirus scan server port number** field, enter the port on which the antivirus scan server listens.

This port number must match the port number of the selected antivirus scan server, specified in the Global_Antivirus_Configuration for that scan server.

7 To block messages if the antivirus scan server is not available for scanning, check the **Block traffic if server is unavailable** check box.

If you select **Block traffic if server is unavailable** and the proxy is unable to contact the antivirus scan server for scanning, the proxy does not forward the file to the intended destination. The requesting user receives an error message.

8 Use the **Scan Options** list to select how scanned files are handled:

- **Scan and Log:** When a virus is detected during scanning, a log entry is generated. No repair is attempted, and the file or message is forwarded to the intended destination.

- **Scan and Delete:** When a virus is detected, the infected file is deleted (no repair is attempted), and a log entry is generated.
- **Scan and Repair or Delete:** When a virus is detected, the antivirus scan server attempts to repair the infected file. Infected files that cannot be repaired are deleted, and a log entry is generated for each deleted file.

9 Use the **Which file extensions to scan** drop-down list to select the file types that will be sent to the antivirus scan server for scanning. The scan server uses these lists to determine what to scan when there are container files.

Your choices are:

- **All files:** All files regardless of extension are sent to the antivirus scan server for scanning.
- **Only those in include list:** Only files with the extensions listed in the include list are sent to the antivirus scan server. If you select this option, you can edit the Include list to add or delete file extensions. The default Include list contains those file types considered at risk of infection.
- **All except those in exclude list:** All files except those with the extensions listed in the Exclude list are sent to the antivirus scan server. If you select this option, you can edit the Exclude list to add or delete file extensions. The default list includes those file types not likely to be infected.

Note: The default Include and Exclude lists contain the recommended file types to protect your network against viruses and other types of malicious code. To minimize potential exposure to infection, use care in editing extension lists. For maximum security, you can choose to scan all file types regardless of extension, but be aware that performance may be impacted during periods of peak usage.

---

10 If you have selected Only those in include list from the Which file extensions to scan list, optionally edit the **Include list** to add or remove file extensions. Add any additional file extensions you want to scan. Delete any extensions that you do not want to scan.

- Use a semicolon (;) to separate file extensions.
- Use a single period to indicate a file without an extension.
- Use a question mark (?) as a wildcard.

If you make changes to the list of included files and want to restore the default list of files, click **Restore default list**.

11 If you have selected All except those in exclude list from the Which file extensions to scan list, optionally edit the **Exclude list** to add or remove file

extensions. Add any file extensions you do not want to scan. Delete any extensions that you want to scan.

- Use a semicolon (;) to separate file extensions.
- Use a single period to indicate a file without an extension.
- Use a question mark (?) as a wildcard.

12 Click **OK** to save your configuration.

Configuring antivirus scanning for the SMTP proxy

The Proxy Services configuration you set up for SMTPD determines how virus scanning is implemented for all rules for which SMTP is enabled as a Service and for which antivirus scanning is enabled.

To configure the antivirus settings for SMTP

1 In the left pane, expand the **Access Controls** node.

2 Click **Proxy Services**.

3 In the right pane, double click **SMTPD** to display the SMTPD Proxy Properties page.

4 Click the **Antivirus Scanning** tab.

Use this tab to control the behavior of virus scanning.

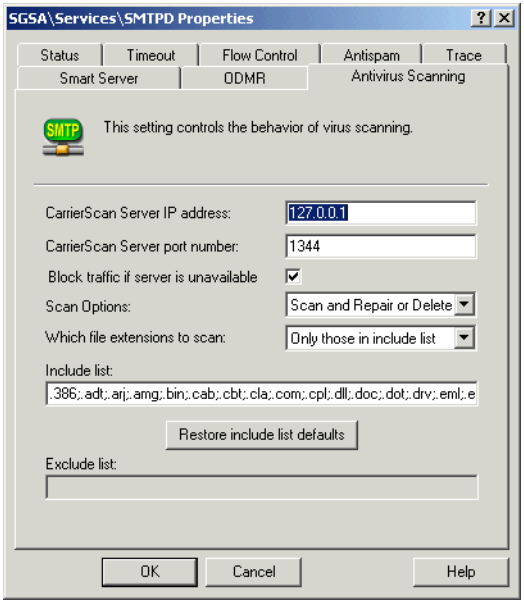


Figure 9-4 SMTPD Properties – Antivirus Scanning Tab

5 In the **Antivirus scan server IP address** field, enter the IP address of the antivirus scan server that will be used to scan for viruses.

The bind address you select here is dependent on whether you want local or remote scanning and on how the antivirus scan server that will do the scanning has been configured. Use the following table for guidance.

Table 9-2 Configure the antivirus settings for SMTP

Configuration	Bind address selected under antivirus scan server global config	Scan server IP address selected here for proxy configuration
The antivirus scan server and the proxy are on the same appliance, and the scan server is configured to accept only local connections	127.0.0.1 (the loopback interface)	127.0.0.1 (the loopback interface)
The antivirus scan server and the proxy are on the same appliance, and the scan server is configured to accept both local and remote connections	0.0.0.0, eth1, or eth0	The physical IP address of the appliance running both the proxy and the antivirus scan server
The proxy will request scanning from an antivirus scan server on a different appliance (thus, that scan server is configured to accept remote connections from this appliance)	0.0.0.0, eth1, or eth0	The physical IP address of the appliance running the antivirus scan server

6 In the **Antivirus scan server port number** field, enter the port on which the antivirus scan server listens.

This port number must match the port number of the selected antivirus scan server, specified in the Global_Antivirus_Configuration for that scan server.

7 To block messages if the antivirus scan server is not available for scanning, check the **Block traffic if server is unavailable** check box.

Note: If you select **Block traffic if server is unavailable** and the proxy is unable to contact the antivirus scan server for scanning, the message is rejected. The message is not forwarded to the intended destination, and an error message is returned indicating that the message was rejected because the antivirus scanner was not available.

8 Use the **Scan Options** list to select how scanned files are handled:

Scan and Log: When a virus is detected during scanning, a log entry is generated. No repair is attempted, and the file or message is forwarded to the intended destination.

Scan and Delete: When a virus is detected, the infected file is deleted (no repair is attempted), and a log entry is generated.

Scan and Repair or Delete: When a virus is detected, the antivirus scan server attempts to repair the infected file. Infected files that cannot be repaired are deleted, and a log entry is generated for each deleted file.

Note: Correct functionality of the settings under Mail Options is dependent on this SMTP Scan Options setting. If you plan to use some or all of the mail filtering capabilities, you must select Scan and Delete or Scan and Repair or Delete here.

---

9 Use the **Which file extensions to scan** drop-down list to select the file types that will be sent to the antivirus scan server for scanning.

Your choices are:

All files: All files regardless of extension are sent to the antivirus scan server for scanning.

Only those in include list: Only files with the extensions listed in the include list are sent to the antivirus scan server. If you select this option, you can edit the Include list to add or delete file extensions. The default Include list contains those file types considered at risk of infection.

All except those in exclude list: All files except those with the extensions listed in the Exclude list are sent to the antivirus scan server. If you select this option, you can edit the Exclude list to add or delete file extensions. The default list includes those file types not likely to be infected.

Note: The default Include and Exclude lists contain the recommended file types to protect your network against viruses and other types of malicious code. To minimize potential exposure to infection, use care in editing extension lists. For maximum security, you can choose to scan all file types regardless of extension, but be aware that performance can be impacted during periods of peak usage.

---

10 If you have selected Only those in include list from the Which file extensions to scan list, optionally edit the **Include list** to add or remove file extensions. Add any additional file extensions you want to scan. Delete any extensions that you do not want to scan.

- Use a semicolon (;) to separate file extensions.

- Use a single period to indicate a file without an extension.
- Use a question mark (?) as a wildcard.

If you make changes to the list of included files and want to restore the default list of files, click **Restore default list**.

11 If you have selected All except those in exclude list from the Which file extensions to scan list, optionally edit the **Exclude list** to add or remove file extensions. Add any file extensions you do not want to scan. Delete any extensions that you want to scan.

- Use a semicolon (;) to separate file extensions.
- Use a single period to indicate a file without an extension.
- Use a question mark (?) as a wildcard.

12 Click **OK** to save your configuration.

Enabling antivirus scanning in a rule

To enable antivirus scanning for the FTP, HTTP, or SMTP proxy in a rule, you must enable the appropriate proxy as a service and make sure that application data scanning is enabled in the rule.

To create a rule with antivirus scanning enabled

1. In the left pane, expand the **Access Controls** node.
2. Right click **Rules** and choose **New** > **Rule** to display the Rule Properties page.
3. Write the rule in accordance with the chapter on Rules in the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.
4. Click the **Miscellaneous** tab.
5. Make sure that the **Application Data Scanning** check box is checked.
6. Click the **Services** tab.

   To configure the FTP proxy for antivirus scanning

   a. Select **ftp*** from the **Excluded Services** list and use the **>>** button to move it to the **Included Services** list.

   b. Select **ftp*** in the Included Services list and click **Configure** to display the FTP Rule Properties page.

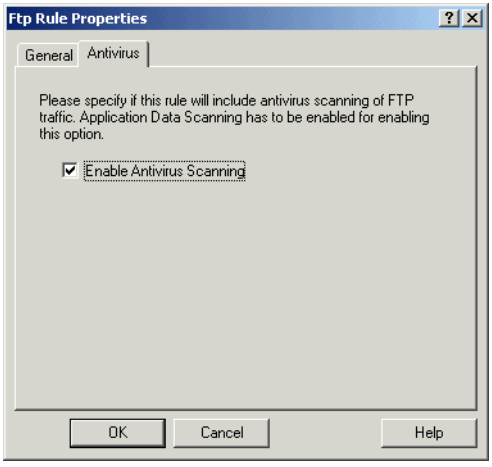

Ftp Rule Properties
General
Antivirus
Please specify if this rule will include antivirus scanning of FTP traffic. Application Data Scanning has to be enabled for enabling this option.
Enable Antivirus Scanning
OK
Cancel
Help

Figure 9-5 FTP Rule Properties Page

   c. Click the **Antivirus** tab.

   d. Check the **Enable Antivirus Scanning** check box.

   e. Click **OK**.

To configure the HTTP proxy for antivirus scanning

a Select **http*** from the **Excluded Services** list and use the **>>** button to move it to the **Included Services** list.

b Select http* in the Included Services list and click **Configure** to display the HTTP Rule Properties page.

c Click the **Antivirus** tab.

d Check the **Enable Antivirus Scanning** check box.

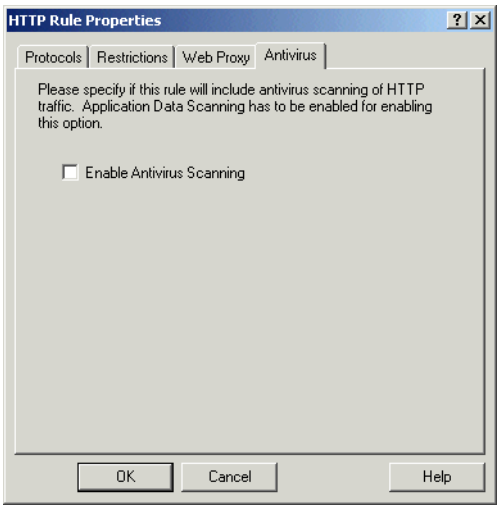


Figure 9-6 HTTP Rule Properties Antivirus page

e Click **OK**.

To configure the SMTP proxy for antivirus scanning

a Select **smtp*** from the **Excluded Services** list and use the **>>** button to move it to the **Included Services** list.

b Select **smtp*** in the **Included Services** list and click **Configure** to display the SMTP Rule Properties page.

c Click the **Antivirus** tab.

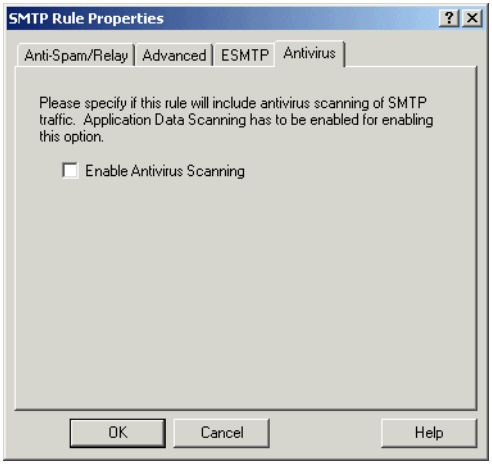


Figure 9-7 SMTP Rule Properties Antivirus Page

d Check the **Enable Antivirus Scanning** check box.

e Click **OK**.

7 When you have finished writing the rule, click **OK** to close the Rule Properties page.

Using the mail filter options

The Mail Options icon under the Antivirus Components node lets you establish a mail policy to filter mail and mail attachments.

You can filter mail based on:

- **File names** - specify one or more file names that are known to be threats, and select whether messages that contain attachments with these file names should be rejected or delivered with the attachment deleted.
- **File size** - specify file sizes of attachments, and select whether messages that contain attachments of the specified size should be rejected or delivered with the attachment removed.
- **Subjects** - specify one or more subject lines that are known to be threats so that messages with these subject lines are rejected.
- **Domains** - specify one or more domains that are known to be threats so that messages from these domains are rejected.
- **Maximum mail size** - specify a maximum size for messages so that messages that exceed the maximum mail size are rejected.
- **Invalid E-mails** - detection of intentionally malformed e-mail messages.
- **Virus Message** - indication of infections in e-mail messages.

Some mail filters can be used during a virus outbreak situation to further protect your network. Once you have information on the characteristics of a new virus, you can use this information to block the infected attachment or e-mail at the appliance. For example, you can use the file name or file size option if you know the exact name or size of an infected attachment. You can protect your network immediately, before virus definitions for the new virus have been posted.

Note: Correct functionality of these mail filtering options is dependent on the Scan Options setting under the antivirus configuration for the SMTP proxy. If you plan to use some or all of the mail filtering capabilities to block mail messages, you must select Scan and Delete or Scan and Repair or Delete as the scan option for SMTP. For more information, see **Configuring antivirus scanning for the SMTP proxy on page 178**.

Filtering mail by attachment file name

When you filter mail by file name, you specify one or more file names that are known to be threats and specify how the antivirus scan server handles messages

that contain attachments with any of the file names listed. The antivirus scan server can reject the entire message or deliver the message with the attachment removed. Any attachments that do not match the listed file names are not removed and are delivered with the message.

For each full file name you want to filter, you enter a separate text string. If the text string you enter matches the file name of any attachment, the message is handled accordingly.

Wildcard characters can be used to match when you are not sure of an exact file name or want to block all attached files with a given extension. For example, to block all attachments with the word virus somewhere in the file name, type *virus* as the subject search string. To block all attachments with the .exe extension, type *.exe.

Note: This filter can be used during in a virus outbreak situation to further protect your network. In the case of a new e-mail-born virus, if you know the file name of the infected attachment, you can use this information to block the infected e-mail at the firewall. You can protect your network immediately, even before virus definitions for the new virus have been posted.

To filter mail based on file name

1. In the left pane, expand the **Antivirus Components** node.
2. Click **Mail Options**.
3. In the right pane, double click **MailFilter_Configuration** to display the MailFilter_Configuration Properties page.

4 Click the **File Names** tab.

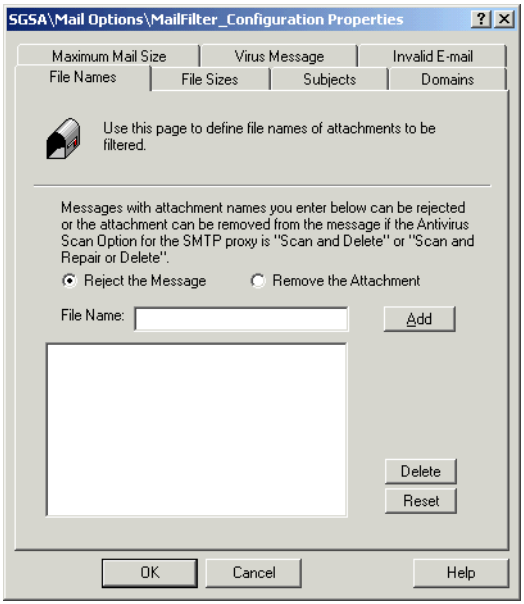

SGSA\Mail Options\MailFilter_Configuration Properties
Maximum Mail Size
Virus Message
Invalid E-mail
File Names
File Sizes
Subjects
Domains
Use this page to define file names of attachments to be filtered.
Messages with attachment names you enter below can be rejected or the attachment can be removed from the message if the Antivirus Scan Option for the SMTP proxy is "Scan and Delete" or "Scan and Repair or Delete".
Reject the Message
Remove the Attachment
File Name:
Add
Delete
Reset
OK
Cancel
Help

Figure 9-8 Mail Filter File Names page

5 Select how the antivirus scan server handles messages that contain an attachment with a specified file name.

Your choices are:

- **Reject the message** - the antivirus scan server rejects all messages that contain an attachment with a specified file name.
- **Remove the attachment** - the antivirus scan server removes any attachments with a specified file name and delivers the rest of the message, including attachments with file names that have not been specified for removal.

6 In the **File Name** field, type a file name.

Search strings are not case sensitive. You can use the following characters:

- Use a question mark (?) as a wildcard to represent a single character.
- Use an asterisk (*) as a wildcard to represent zero or more characters.
- Use a backslash (\) as an escape character. For example, precede ? or * with \ to match a literal ? or * in a file name. To match a literal \, use \\.

7 Click **Add**.

The file name you have specified displays, prefaced by the action the antivirus scan server will take. For example, [Reject Message] love.vba.

The File Name field clears, letting you specify another file name. You can add multiple file names. For each file name you specify, you first select how the antivirus scan server handles messages with attachments that match that file name.

8 To remove a file name from the list, select it in the list and click **Delete**.

9 To start over with a blank list, click **Reset**.

10 When you have finished, click **OK**.

Filtering mail by attachment file size

When you filter mail by attachment file size, you specify one or more file sizes that are known to be threats and specify how the antivirus scan server handles messages that contain attachments of any of the listed file sizes. The antivirus scan server can reject the entire message or deliver the message with the attachment removed (any attachments that are not a listed size are not removed and are delivered with the message).

Note: This filter can be used during in a virus outbreak situation to further protect your network. In the case of a new e-mail-born virus, if you know the exact file size of the infected attachment, you can use this information to block the infected e-mail at the firewall. You can protect your network immediately, even before virus definitions for the new virus have been posted.

To filter mail based on attachment file size

1 In the left pane, expand the **Antivirus Components** node.

2 Click **Mail Options**.

3 In the right pane, double click **MailFilter_Configuration** to display the MailFilter_Configuration Properties page.

4 Click the **File Sizes** tab.

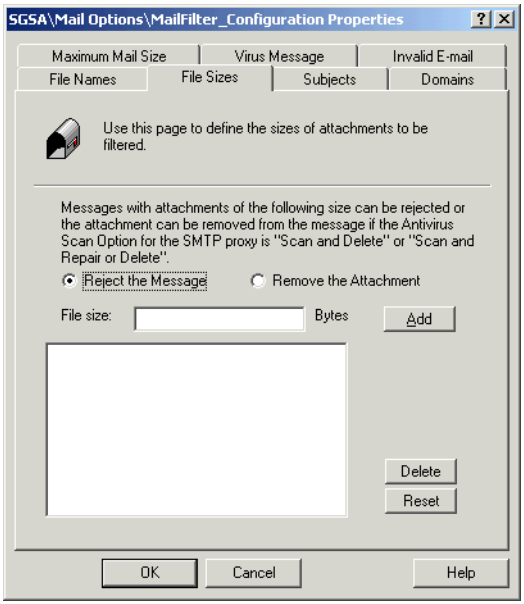

SGSA\Mail Options\MailFilter_Configuration Properties
Maximum Mail Size
Virus Message
Invalid E-mail
File Names
File Sizes
Subjects
Domains
Use this page to define the sizes of attachments to be filtered.
Messages with attachments of the following size can be rejected or the attachment can be removed from the message if the Antivirus Scan Option for the SMTP proxy is "Scan and Delete" or "Scan and Repair or Delete".
Reject the Message
Remove the Attachment
File size:
Bytes
Add
Delete
Reset
OK
Cancel
Help

Figure 9-9 Mail Filter File Sizes page

5 Select how the antivirus scan server will handle messages than contain an attachment of a size you have specified.

Your choices are:

- **Reject the message** - the antivirus scan server rejects messages that contain an attachment of a specified size.
- **Remove the attachment** - the antivirus scan server removes any attachments of a specified size and delivers the rest of the message, including attachments that have not been specified for removal.

6 In the **File size** field, enter a file size (in bytes).

7 Click **Add**.

The file size you have specified displays, prefaced by the action the antivirus scan server will take. For example, [Reject Message] 20000.

The File size field clears, letting you specify another file size. You can add multiple file sizes. For each file size you specify, you first select how the antivirus scan server handles messages with attachments that match that file size.

8 To remove a file size from the list, select it in the list and click **Delete**.

9 To start over with a blank list, click **Reset**.

10 When you have finished, click **OK**.

You can also configure the antivirus scan server to reject messages that exceed a maximum size limit. For more information, see **Filtering mail by maximum mail size on page 195**.

Filtering mail by subject

To filter by subject, you specify one or more subject lines (or strings to be found within subject lines) that are known to be threats. Messages with these subject lines are rejected.

Subject strings you specify are matched against the subject line of each e-mail. Wildcard characters can be used appropriately to match when you are not sure of the exact subject line. Any white space (tabs or spaces) at the beginning of the subject line is ignored. White space at the beginning of your search string (the text you enter for the subject line filter) is also ignored. White space at the end of the subject line and search string is not ignored. For example if you specify “block me” in a subject line, “block me “ will not be blocked.

Note: This filter can be used during in a virus outbreak situation to further protect your network. In the case of a new e-mail-born virus, if you know the subject line or part of the subject line of the infected message, you can use this information to block infected e-mail at the firewall. You can protect your network immediately, even before virus definitions for the new virus have been posted.

To filter mail based on subject

1 In the left pane, expand the **Antivirus Components** node.

2 Click **Mail Options**.

3 In the right pane, double click **MailFilter_Configuration** to display the MailFilter_Configuration Properties page.

4 Click the **Subjects** tab.

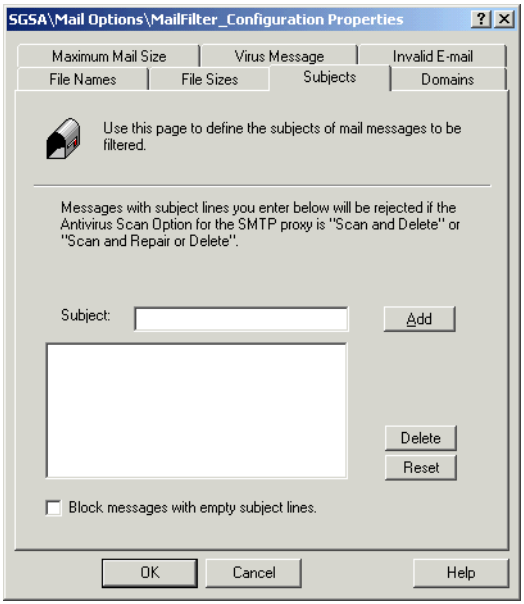


Figure 9-10 Mail Filter Subjects page

5 In the **Subject** field, type a text string.

Search strings are not case sensitive. You can use the following characters:

- Use a question mark (?) as a wildcard to represent a single character.
- Use an asterisk (*) as a wildcard to represent zero or more characters.
- Use a backslash (\) as an escape character. For example, precede ? or * with \ to match a literal ? or * in a file name. To match a literal \, use \\.

6 Click **Add**.

The text string displays in the list.

The Subject field clears, letting you enter another text string. You can add multiple subjects.

7 To remove a subject from the list, select it in the list and click **Delete**.

8 To start over with a blank list, click **Reset**.

9 To filter mail messages that have a blank subject line, check the **Block messages with empty subject lines** check box.

10 When you have finished, click **OK**.

Filtering mail by domain

To filter by domain, you specify one or more domain names that are known to be threats. The domain name search string that you enter is matched against addresses in the From header of the e-mail message. If the search string matches an address, the message is rejected.

You can use this filter to block mail from specific e-mail addresses, as well as mail from a specific domain. Wildcard characters can be used as necessary to control exactly what you want to block. For example:

- Using: *@somedomain.com
  blocks: smith@somedomain.com
  but does not block: smith@someserver.somedomain.com
- Using: *@*somedomain.com
  or using: *somedomain.com
  blocks: smith@somedomain.com
  and blocks: smith@someserver.somedomain.com

For blocking specific e-mail addresses:

- Using: smith@somedomain.com
  blocks only: smith@somedomain.com
  but does not block: adam_smith@somedomain.com
  or block: smith@someserver.somedomain.com

To filter mail based on domain

1. In the left pane, expand the **Antivirus Components** node.
2. Click **Mail Options**.
3. In the right pane, double click **MailFilter_Configuration** to display the MailFilter_Configuration Properties page.

4 Click the **Domains** tab.

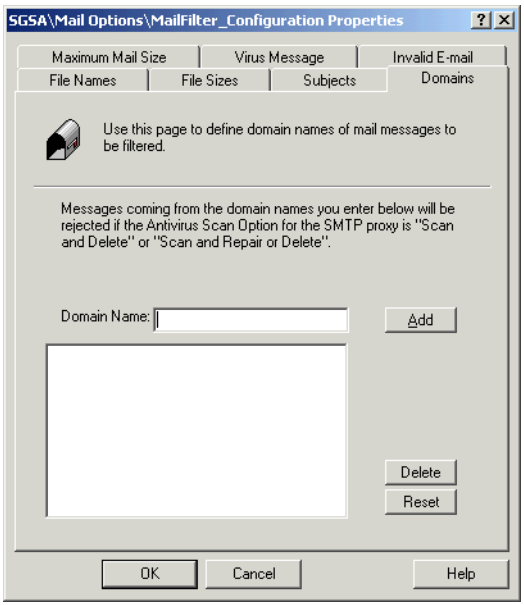

SGSA\Mail Options\MailFilter_Configuration Properties
Maximum Mail Size
Virus Message
Invalid E-mail
File Names
File Sizes
Subjects
Domains
Use this page to define domain names of mail messages to be filtered.
Messages coming from the domain names you enter below will be rejected if the Antivirus Scan Option for the SMTP proxy is "Scan and Delete" or "Scan and Repair or Delete".
Domain Name:
Add
Delete
Reset
OK
Cancel
Help

Figure 9-11 Mail Filter Domains page

5 In the **Domain** field, type a text string.

Search strings are not case sensitive. You can use the following characters:

- Use a question mark (?) as a wildcard to represent a single character.
- Use an asterisk (*) as a wildcard to represent zero or more characters.
- Use a backslash (\) as an escape character. For example, precede ? or * with \ to match a literal ? or * in a file name. To match a literal \, use \\.

6 Click **Add**.

The domain displays in the list.

The Domain name field clears, letting you enter another domain name. You can add multiple domain names.

7 To remove a domain name from the list, select it in the list and click **Delete**.

8 To start over with a blank list, click **Reset**.

9 When you have finished, click **OK**.

Filtering mail by maximum mail size

You can specify a maximum size for mail messages. This maximum size includes the entire message including any and all attachments. Messages that exceed this maximum mail size are rejected.

A value of 0 (the default value) indicates no maximum size. By default, no messages are rejected based on maximum size.

To filter mail based on maximum mail size

1. In the left pane, expand the **Antivirus Components** node.
2. Click **Mail Options**.
3. In the right pane, double click **MailFilter_Configuration** to display the MailFilter_Configuration Properties page.
4. Click the **Maximum Mail Size** tab.

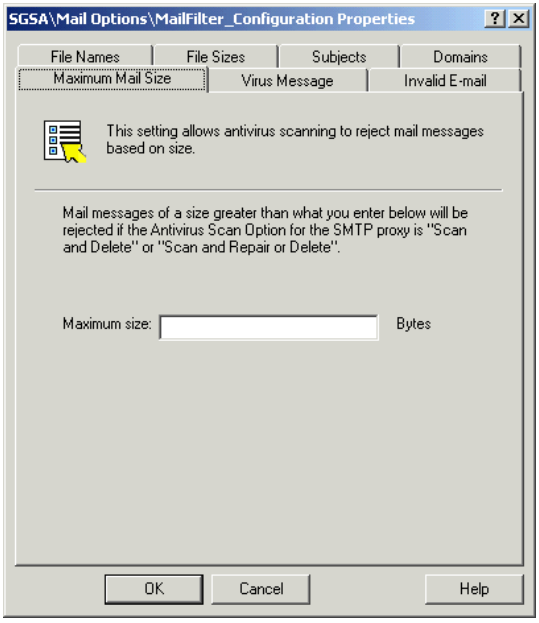

SGSA\Mail Options\MailFilter_Configuration Properties
File Names
File Sizes
Subjects
Domains
Maximum Mail Size
Virus Message
Invalid E-mail
This setting allows antivirus scanning to reject mail messages based on size.
Mail messages of a size greater than what you enter below will be rejected if the Antivirus Scan Option for the SMTP proxy is "Scan and Delete" or "Scan and Repair or Delete".
Maximum size:
Bytes
OK
Cancel
Help

Figure 9-12 Mail Filter Maximum Mail Size page

5. In the **Maximum size** field, enter the maximum mail size (in bytes) that the appliance will accept.

   Use a 0 (this is the default value) to indicate no maximum.
6. Click **OK**.

Rejecting invalid mail messages

Computer viruses and malicious programs sometimes create intentionally malformed e-mail messages. These distortions are recognized by the antivirus scan server and can be used as criteria to reject potentially infected messages.

To reject invalid mail messages

1. In the left pane, expand the **Antivirus Components** node.
2. Click **Mail Options**.
3. In the right pane, double click **MailFilter_Configuration** to display the MailFilter_Configuration Properties page.
4. Click the **Invalid E-mail** tab.

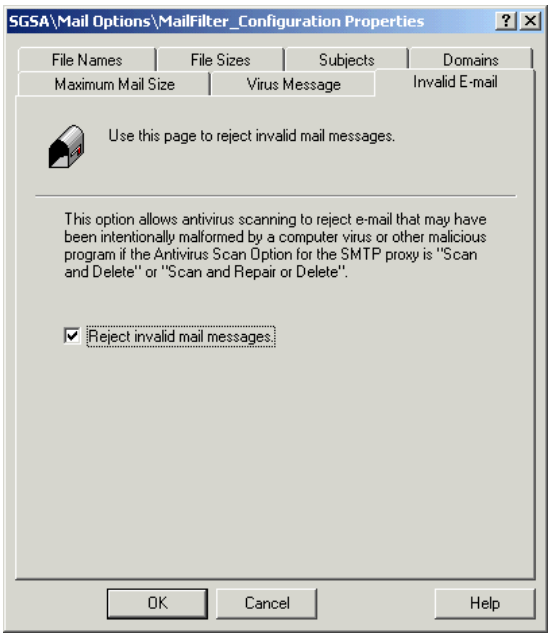

SGSA\Mail Options\MailFilter_Configuration Properties
File Names
File Sizes
Subjects
Domains
Maximum Mail Size
Virus Message
Invalid E-mail
Use this page to reject invalid mail messages.
This option allows antivirus scanning to reject e-mail that may have been intentionally malformed by a computer virus or other malicious program if the Antivirus Scan Option for the SMTP proxy is "Scan and Delete" or "Scan and Repair or Delete".
Reject invalid mail messages
OK
Cancel
Help

Figure 9-13 Mail Filter Invalid E-mail page

5. Check the **Reject invalid mail messages** check box.
6. Click **OK**.

Customizing virus messages

When an infection is found (and repaired or deleted) in a MIME-encoded message scanned by the antivirus scan server, the antivirus scan server can be configured to add two types of messages to the mail message to warn the recipient that a virus was found. Default text is provided. Either or both messages can be customized.

You can customize:

- The file repair message, which is added to the body of an e-mail message when an infected attachment is repaired or is deleted because it contained an unrepairable virus or because it violated the established mail policy

  For more information, see **Editing the File Repair Message on page 198**.

- The file remove message, which is placed in a text file called infection.txt and attached to an e-mail message in place of an infected attachment that must be deleted because it cannot be repaired

  The file remove message is used only when an attachment is removed because it contains a virus. It is not used when the attachment is removed because of a mail policy violation.

  For more information, see **Editing the File Remove Message on page 200**.

To update e-mail messages when an infected file is repaired or deleted

1. In the left pane, expand the **Antivirus Components** node.
2. Click **Mail Options**.
3. In the right pane, double click **MailFilter_Configuration** to display the MailFilter_Configuration Properties page.

4 Click the **Virus Message** tab.

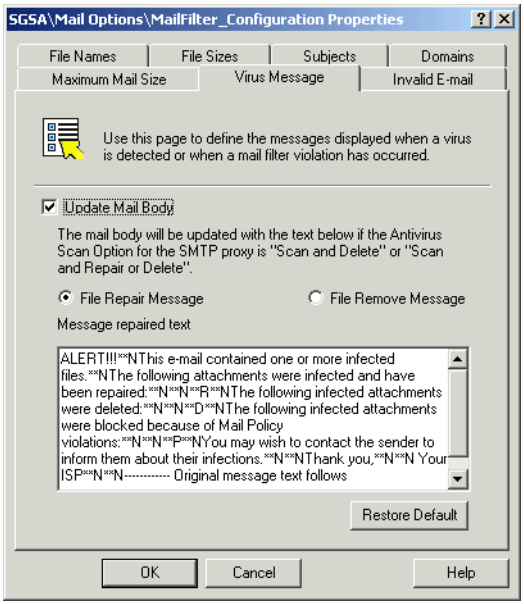

SGSA\Mail Options\MailFilter_Configuration Properties
File Names
File Sizes
Subjects
Domains
Maximum Mail Size
Virus Message
Invalid E-mail
Use this page to define the messages displayed when a virus is detected or when a mail filter violation has occurred.
Update Mail Body
The mail body will be updated with the text below if the Antivirus Scan Option for the SMTP proxy is "Scan and Delete" or "Scan and Repair or Delete".
File Repair Message
File Remove Message
Message repaired text
ALERT!!!**NThis e-mail contained one or more infected files.**NThe following attachments were infected and have been repaired:**N**N**R**NThe following infected attachments were deleted:**N**N**D**NThe following infected attachments were blocked because of Mail Policy violations:**N**N**P**NYou may wish to contact the sender to inform them about their infections.**N**NThank you,**N**N Your ISP**N**N---------- Original message text follows
Restore Default
OK
Cancel
Help

Figure 9-14 Mail Filter Virus Message page

5 Check the **Update Mail body** check box.

6 To optionally customize a message, click either the **File Repair Message** or the **File Remove Message** radio button.

The text of the selected message displays in the text box.

7 Edit the message as necessary.

For more information, see **Editing the File Repair Message on page 198** or **Editing the File Remove Message on page 200**.

To restore the original text of the message, click **Restore Default**.

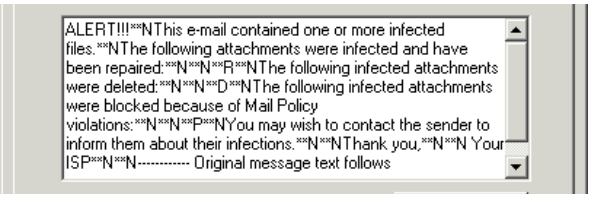
8 Click **OK** to save your configuration.

Editing the File Repair Message

The File Repair Message is added to the body of an e-mail message when an infected attachment is repaired or is deleted because it contained an unrepairable virus or because it violated the established mail policy.

Several variables can be used as needed to customize the File Repair Message. These variables are described below. When editing the message, you can edit both the text and the variables.

Message as it appears with variables:


ALERT!!!**NThis e-mail contained one or more infected files.**NThe following attachments were infected and have been repaired:**N**N**R**NThe following infected attachments were deleted:**N**N**D**NThe following infected attachments were blocked because of Mail Policy violations:**N**N**P**NYou may wish to contact the sender to inform them about their infections.**N**NThank you,**N**N Your ISP**N**N---------- Original message text follows

Message text as it appears to the user:

```
ALERT!!!
This email contained one or more infected files.
The following attachments were infected and have been
repaired:

<list of infected files>

The following infected attachments were deleted:

<list of deleted files>

The following attachments were blocked because of Mail
Policy violations:

<list of blocked files>

You may wish to contact the sender to inform them about
their infections.

Thank you,

Your ISP

---------- Original message text follows ------------
```

The following variables can be used to customize File Repair Message text:

Table 9-3 Variables used to customize the File Repair Message

Variable	Description
**N	Moves to the next line
**R	Displays a list of all infected attachments for a given message that have been repaired
**D	Displays a list of all infected attachments for a given message that have been deleted because they could not be repaired
**I	Displays a list of all infected attachments for a given message that were identified, whether deleted or repaired
**P	Displays a list of all attachments that were blocked because of a mail policy violation

Editing the File Remove Message

The File Remove Message is placed in a text file called infection.txt and attached to an e-mail message in place of an infected attachment that is deleted because it cannot be repaired. The file remove message is used only to replace an attachment that is removed because it contains a virus and not when the attachment is removed because of a mail policy violation.

To edit this message, simply change the text. Message text as it appears to the user:

```
A file was removed because it contained malicious code
that could not be removed.
```

Chapter 10

Content Filtering

The Symantec Gateway Security appliance provides flexible internet content filtering technology. This increases worker productivity and preserves valuable bandwidth by focusing web access on business related content. At the same time, it decreases exposure to liability by restricting access to potentially objectionable content. URL filtering can be configured on a global, per user, per user group, per IP or per IP group basis.

Using content profiles

The Symantec Gateway Security appliance enables you to restrict certain classes of URLs based on a website ratings service. This service, called the WebNOT Ratings Service, provides subscribers with frequently updated ratings database of URLs that are categorized by topic. New updates are downloaded automatically to the appliance from the WebNOT site on the internet. A subscription to WebNOT is included with the Symantec Gateway Security appliance Gold and Platinum support contracts.

The Symantec Gateway Security appliance also comes with a pre-installed WebNOT ratings list database to enable content filtering as soon as the appliance is installed and configured. The pre-installed database is fully functional and useful for evaluation purposes; however, it is a version based on the ship date of the appliance. It is updated to the latest version within 24 hours after you install the appliance with the product key. The WebNOT database is checked daily and updated whenever changes are made.

Caution: Do not enable ratings for rules with HTTP if you do not have a ratings list database. Otherwise, all HTTP requests that use the rule will be denied.

Creating rating rule profiles

To create a ratings profile

1. Expand the **Access Controls** folder.
2. Select the **Content Profiles** folder and double click to expand it.
3. Double click the **Rating Rule Profiles** folder to expand it and display the Rating Profiles and Rating Modifications icons in the right pane.
4. Select the **Rating Profiles** icon.
5. Right click and select **New>Rating Profile** from the Action menu to display the Rating Profile Properties page (see **Figure 10-2**).

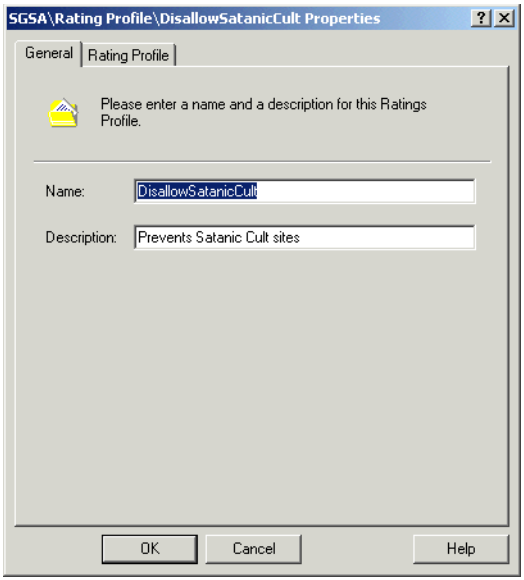


Figure 10-1 Rating Profiles Properties - General tab

6 In the **General** tab, enter a name in the **Name** field.

This is the name that becomes accessible from the Ratings Rule Properties page.

7 Enter a description of your profile.

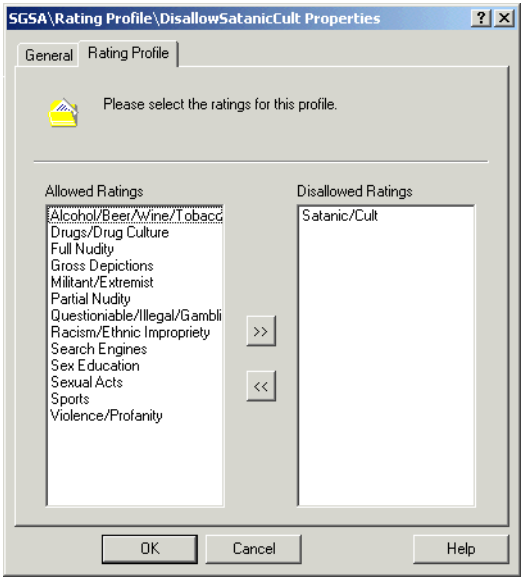


Figure 10-2 Rating Profiles Properties - Rating Profile tab

8 Select the **Rating Profile** tab.

9 In the **Allowed Ratings** field, click on the name of a topic you want to include in your profile and use the right arrow to move it to the **Disallowed Ratings** field (these are topics you are planning to ban).

To select multiple topics, press and hold the **Shift** key while clicking.

10 Click **OK** to save your profile.

The WebNOT profiles created in this way appear in a dialog window when you select **ratings*** in the SRMC Rule Properties page and click the **Configure...** button. Ratings profiles are applied to the HTTP protocol selected in the same rule as the ratings service.

Using a ratings profile in a rule

To use a ratings profile in a rule

1 Expand the **Access Controls** folder.

2 Select the **Rules** icon, right click, and choose **New>Rule**.

The Rule Properties page is displayed.

3 Create your rule following the guidelines in the section on Rules in the *Symantec Enterprise Firewall and Symantec Enterprise VPN Configuration Guide*.

4 Select the **Services** Tab.

5 Select **ratings*** from the **Excluded Services** list and move it to the **Included Services** list by using the >> button.

6 Click the **Configure...** button.

The Ratings Rule Properties dialog box opens as shown in **Figure 10-3**. This dialog box allows you to select an existing profile to use in a rule. A ratings profile is a list of topics grouped together under one name or profile. These profiles are used to determine which URLs are blocked.

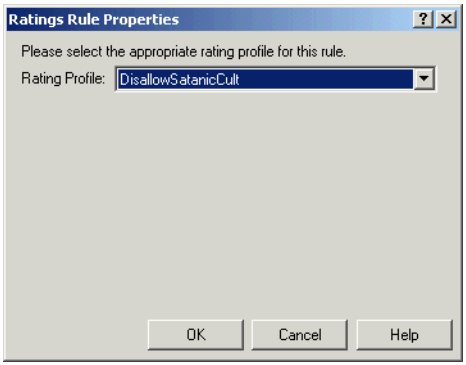


Figure 10-3 Ratings Rule Properties Page

7 Select a profile from the drop down menu.

8 Click the **OK** button to assign the Rating Profile to the rule.

9 Click **OK** in the Rule Properties page to save the Rule.

Searching capabilities

You can search for specific URLs among the extensive database of rated URLs from the Ratings Modifications Properties page, under the Rating Rule Profiles icon.

To locate a specific URL in the Ratings database

1 Expand the **Access Controls** folder. Select the **Content Profiles** folder and double click to expand it.

2 Double click the **Rating Rule Profiles** folder.

The Ratings Profiles and Rating Modifications icons appears in the right pane.

3 Select the **Ratings Modifications** icon.

4 Right click and select **All Tasks**>**Search** to open the Ratings Modifications URL dialog box.

5 Key in the URL you are searching for in the ratings database.

You can enter the entire URL or the IP address.

6 Click the **OK** button.

The search process may take several seconds. Once your URL is found, you can edit its rating.

Customizing WebNOT ratings lists

You can customize your ratings lists, changing the categories to which web sites, news groups, and Gopher sites belong. This feature allows you to adjust for special circumstances.

For example, suppose your company prohibits sites rated as **Sports**. However, your company does considerable business in the Arctic Ocean and needs to refer to a site called www.arctic_ocean.com, which, for whatever reason, is rated as **Sports**.

To modify the rating

1 Located the URL you want to modify using the previous procedure (See Searching capabilities on page 205).

Once the URL is located, it appears in the **Location** field of the Ratings Modifications Property page, ready for editing. For this example: *http://www.arctic_ocean.com.*

2 Enter a description of the location. For example: *Site dealing with economic development in the Arctic region*.

3 Select the **Rating Modification** tab.

4 Select **Sports** in the **Ratings** field and use the >> button to move it to the **Location rated as** field.

5 Click **OK.**

You can also add categories to a site's Ratings list. Prefix Web sites with **http:// .**

Using content restrictions

HTTP Document Content restrictions, accessible via the **Access Controls/ Content Profiles** folder, allow you to control access to web content according to file extension, URL, and by MIME type.

Allowing extensions

You can use the **Allow Extensions** service limitation to allow access only to files with specific extensions that you designate. For example, you may wish to allow access only to HTML and graphics files to better control the types of data transferred through your Internet connection.

Caution: This service limitation is very restrictive, since all file extensions not listed in the file are denied by the host system.

To create a list of allowable filename extensions for HTTP rules

1 Expand the **Access Controls** folder.

Select the **Content Profiles** folder in the SRMC and double click to expand it.

2 Select the **HTTP Document Content** icon. Right click and select **New>Extension** to display the Extensions Properties page, as shown in Figure 10-4.

.

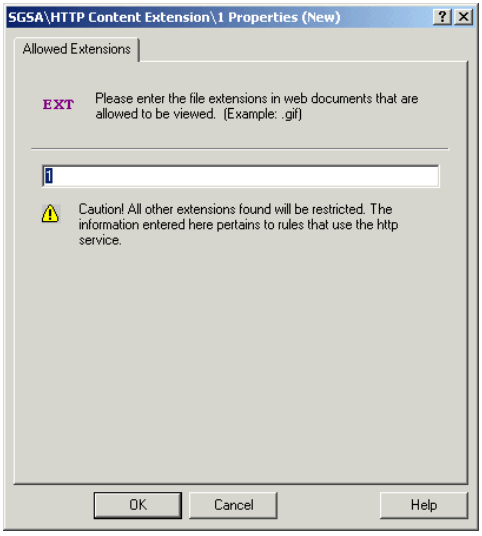

SGSA\HTTP Content Extension\1 Properties (New)
Allowed Extensions
EXT
Please enter the file extensions in web documents that are allowed to be viewed. (Example: .gif)
1
Caution! All other extensions found will be restricted. The information entered here pertains to rules that use the http service.
OK
Cancel
Help

Figure 10-4 HTTP Content Extension Properties Page

3 In the provided field, enter the extensions you wish to allow (for example `.gif,.txt`).

Enter several extensions at once, separated by a space or enter one at a time. Any extensions not listed are then disallowed if you create a rule that restricts the HTTP proxy by file extensions.

4 When finished, click the **OK** button in the properties page.

Allowing URLs

For ordinary HTTP services, you can use the Allow URLs service limitation to allow access only to specific URLs.

Caution: This service limitation is very restrictive, since all URLs not are not specified as allowed are denied by the host system.

To create a list of allowable URLs for HTTP rules

1 Expand the **Access Controls** folder.

2 Select the **Content Profiles** folder and double click to expand it.

3 Right click the **HTTP Document Content** icon and select **New>URL** from the menu.

4 In the **Allowed URLs** Property page, enter a URL you wish to allow in the provided field. The wildcard "*" is permitted as the last character in an entry and permits any URL that matches the characters before it.

The following are sample entries:

```
http://xyz.abc.com/intro/overview.html
```

```
http://foo.bar.edu/salestuff/*
```

The wildcard can only be used as the last element of a pathname in a URL. It cannot be used as part of a host name. The following examples will not work.

```
http://xyz.*(used in the host portion of the URL)
```

```
http://xyz.abc.com/*/overview.html (not final)
```

5 When finished, click **OK**.

You must create a separate allowed URL for each URL you want to allow. Repeat steps 1 through 4.

All rules employing this service limitation only allow HTTP access to the URLs that are specified as allowed. Users will only be able to access and retrieve information from URLs listed. Access to all other URLs is blocked.

Note: Transparent connections match against the reverse-mapped DNS name of the requested address. To allow transparent access, you must include the reverse-mapped address in the `httpurls` file. If reverse lookups are disabled, use the IP address.

HTTP restrictions in a rule

To specify HTTP restrictions in a rule

1 Expand the **Access Controls** folder and click on **Rules**.

2 Right click and choose **New>Rule** to create a new rule or double click on an existing rule to display its Properties page.

3 Click the **Services** tab.

If http* is not listed as an included service, select it in the **Excluded Services** list and use the >> key to move it to the **Included Services** list.

4 With http* selected, click **Configure**.

5 Click the **Restrictions** tab, and check one or both of the following:

- **Restrict By URLs** - Select this option if you subscribe to the WebNOT service or to block designated URLs.
- **Restrict By File Extensions** - Select this option if you have entered only specific file extensions to be allowed in the Allowed Extensions tab of the HTTP Content Extensions Properties page.

6 Click **OK**.

HTTP URL patterns

HTTP URL patterning can be used to protect a web server from being accessed illegally by the use of special characters in the incoming URL string.

To prevent this from happening, the appliance includes a file named httpurlpattern.cf. This file contains a list of potentially harmful regular expressions that can be used to try to hack into your server. When incoming URLs are checked against this file, access via these "url patterns" is denied.

To initiate a check of this file, you must do three things:

- Determine the weaknesses against which you want to defend. These are frequently published by organizations such as Network Security Focus at http://www.nsfocus.com or by third party products to prevent attacks through weaknesses in their software.
- Edit the httpurlpattern.cf file to specify the regular expression that should be rejected.

  Many URL patterns are defined in this file. You can make this file more generic or more specific based on the needs of your environment. For more information about editing this file, see the *Symantec Enterprise Firewall and Symantec Enterprise VPN Reference Guide*.
- Create a rule for HTTP access that will check incoming URLs against the list in httpurlpattern.cf.

To create a rule using http url patterning

1 Create a new rule.

2 From the **Services** tab, choose http* as the service.

3 From the **Advanced Services** tab, click **Add** to display the Service Parameters dialog box.

4 Enter http.urlpattern in the parameter field, then click **OK**.

Examples:

- If you have a public server www.xyz.com, all documents you serve are stored under that default directory. Someone trying to penetrate your network could use the string www.xyz.com/../ to access the parent directory of your document directory if your server is not properly configured and secured.

  If the pattern '../' is present in the httpurlpattern.cf file, such an access will be blocked yet legal accesses are not affected.

- The unpatched version of a product ships with an insecure script, faxsurvey, which allows remote command execution with the privileges of the web server process. This can be exploited simply by passing the command as a parameter to the script.

  For example, an attacker could use the following URL to get your system information:

  ```
  http://www.yoursite.com/cgi-bin/
  faxsurvey?uname%20%20da
  ```

  They could use the following URL to get a copy of your password file:

  ```
  http://www.yoursite.com/cgi-bin/faxsurvey?/bin/
  cat%20/etc/passwd
  ```

  Note: %20 and %2d are not regular expressions. They are the encoding of ISO Latin 1, representing a space and - , respectively.

Denying MIME types

You can restrict access to files based on Multipurpose Internet Mail Extension (MIME) Types. Unlike service limitations that apply on a per-rule basis, MIME restrictions apply globally to all http-based services. Use this feature to prevent downloading of certain usage formats (such as graphics files) or application types.

To limit MIME types

1. Expand the **Access Controls** folder and double click the **Content Profiles** folder to expand it.
2. Select the **HTTP Document Content** icon, right click, and choose **New>MIME Type**. The Denied MIME Types Properties page appears.
3. In the text field, enter the MIME type you want to deny, using the following format:

   image/gif

4 Click **OK** to save your entry.

Repeat this procedure for each MIME type you want to restrict. To remove a MIME type, select it and press the Delete key.

Chapter 11

High Availability and Load Balancing

The Symantec Gateway Security appliance provides high availability and load balancing (HA/LB) features. Load balancing allows the members of a cluster to share the work. A special case, or feature, of load balancing is referred to as high availability, meaning that if one appliance fails, the remaining member or members of the cluster can take over and continue to share the load.

HA/LB is an optional feature. You must purchase an HA/LB Crossgrade License for each appliance in a cluster. Check with your system administrator for license requirements.

About the cluster wizard

The Symantec Gateway Security appliance provides a Cluster wizard to group appliances into a cluster for three purposes:

- **Integrated Software HA/LB** - To configure software high availability and load balancing on appliances with HA/LB enabled using built-in clustering functionality.
- **Hardware HA/LB** - To configure hardware high availability and load balancing on appliances with HA/LB enabled that are connected to a Radware FireProof™ device. Radware's FireProof™ is an intelligent traffic management device for multiple firewalls and Virtual Private Network (VPN) devices. See www.radware.com for more information.

  Other third-party hardware HA/LB devices can be used, but are not supported by Symantec. An option is provided to configure third party hardware HA/LB devices.
- **Other replication** - To enable the propagation of configuration files from one appliance to other appliances. Symantec Gateway Security appliance configuration information is stored in the var/lib/sg directory. When you select an appliance in your cluster and click on Propagate, all files from that appliance's sg directory are copied to the sg directories of enabled members of the cluster. This allows all members of the cluster to appear as one appliance, with the same users, network entities, rules, and all other properties.

After you have created a cluster, you can manage it by right clicking the cluster name and choosing one of the following options from the All Tasks menu.

- **Verify Cluster** - Identifies cluster members that may not have the same configuration and allows you to update the configuration based on a selected cluster member.
- **Modify Cluster** - Allows you to add members to a cluster after it is created, to delete members, to change the cluster's control network, and to change virtual IP addresses.

  You can also use the Modify Cluster wizard to enable or disable members of a cluster when you are preparing to propagate configuration changes from one member of a cluster to the rest of the cluster.
- **Delete Cluster** - Allows you to delete the cluster configuration information from all the members of the cluster. This does not delete any appliances. It removes the configuration information that associates them with a cluster.

Preparing to create a cluster

Every Symantec Gateway Security appliance to be added to a cluster must meet the following prerequisites:

- All members must have the same number of configured interfaces.
- All members must run the same operating system version.
- The network configuration of all cluster members must match; every cluster member must have IP addresses on the same subnets as the other cluster members.
- Each appliance must have a different system name.
- HA/LB must be enabled on all appliances

In addition, the IP address specified to connect to the Symantec Gateway Security appliance must lie on the same subnet as the IP addresses specified to connect to the other members.

Before you create a cluster

- Define the IP addresses of all the appliances you want to add to the cluster.
- Define the remote management passwords of all the appliances you want to add to the cluster, using the SRMC.

Creating a cluster for software high availability/load balancing

The following procedure describes how to create a cluster for software or hardware high availability and load balancing (HA/LB).

An HA/LB cluster can also be used to propagate appliance configuration files from one cluster member to all other enabled members of the cluster. See **Creating a cluster for appliance file propagation or hardware HA/LB on page 222**.

Before you create the cluster, make sure that the IP addresses and passwords of all the appliances you want to add to the cluster have been defined on all the appliances that will be added to the cluster.

To create a software HA/LB cluster

1 Click the **Symantec Raptor Management Console** icon to display the Getting Connected taskpad in the right pane.

If the Taskpad is not displayed, pull down the **View** menu and choose **Taskpad**.

2 Click the **New Cluster** icon to display the Create Cluster Wizard.

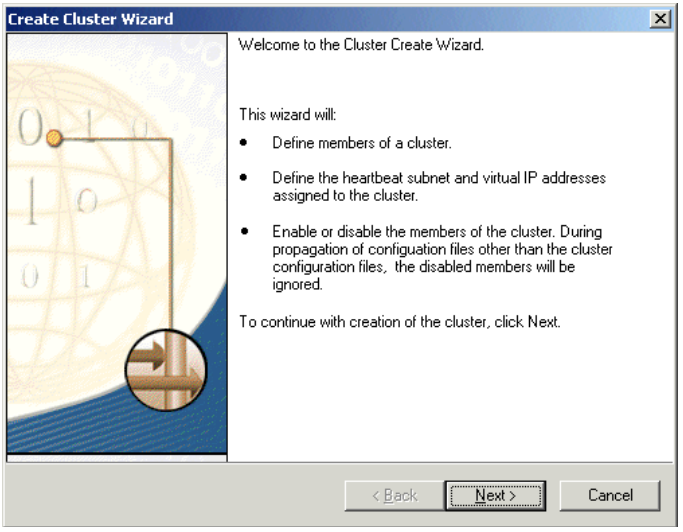

Create Cluster Wizard
Welcome to the Cluster Create Wizard.
This wizard will:
Define members of a cluster.
Define the heartbeat subnet and virtual IP addresses assigned to the cluster.
Enable or disable the members of the cluster. During propagation of configuation files other than the cluster configuration files, the disabled members will be ignored.
To continue with creation of the cluster, click Next.
< Back
Next >
Cancel

Figure 11-1 Create Cluster wizard Introduction screen

3 Click **Next** to display the Create a new cluster screen.

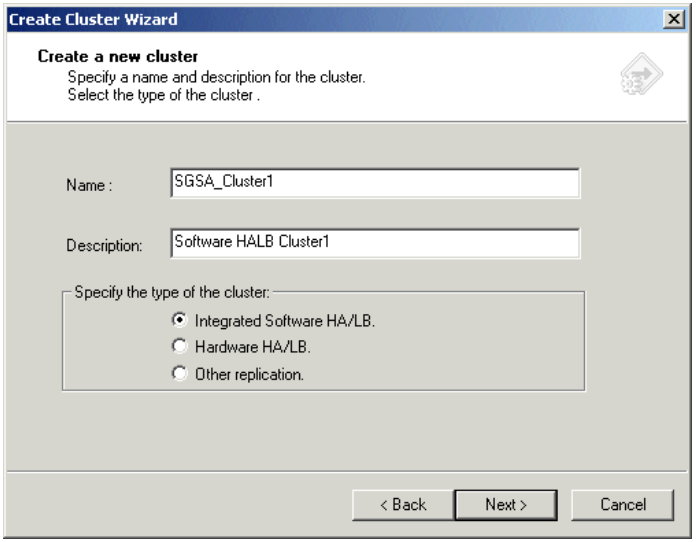


Figure 11-2 Create a new cluster wizard screen

4 Enter a name and description for the cluster.

5 Click the **Integrated Software HA/LB** radio button.

6 Click **Next** to display the Cluster members screen.

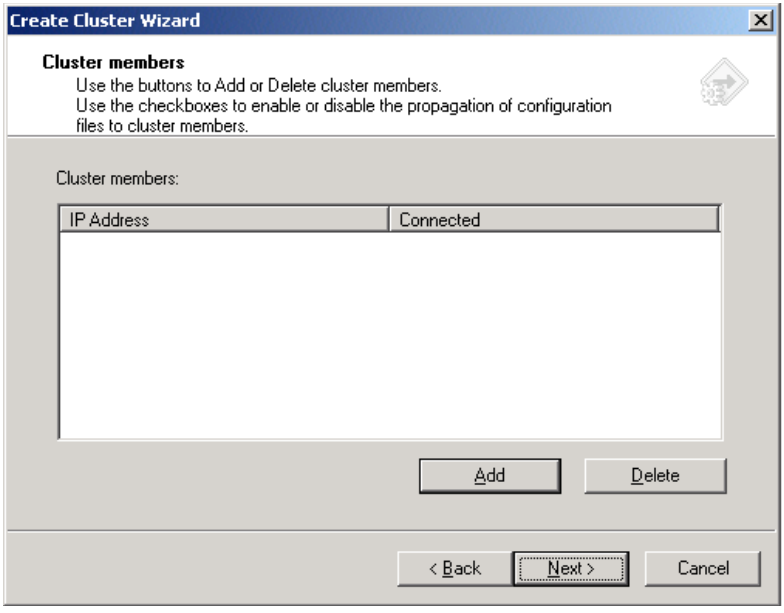


Figure 11-3 Cluster members screen

7 To add the first member to the cluster, click **Add** to display the Connect to cluster member dialog box.

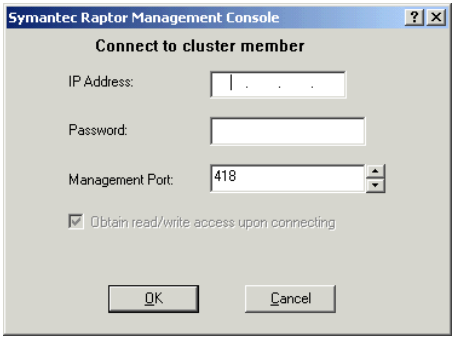


Figure 11-4 Connect to cluster member dialog box

8 Enter the IP address of the appliance that will be the first cluster member, and the password and port number that are used to connect to it.

Note: The **Obtain read/write access** check box is grayed out and cannot be edited. It indicates that when the Cluster Wizard attempts to connect you to the specified appliance, you must be able to obtain read/write access to add the appliance to the cluster.

---

9 Click **OK** and the Cluster wizard will attempt to connect to the appliance.

- If this is the first time this appliance is being added to a cluster, the Cluster members screen is redisplayed, showing the IP address of the appliance and verifying that you are connected.
- If the appliance is already a member of a cluster, a message asks if you want to read the existing cluster information for the appliance.

  If you click **Yes**, the name and description of the cluster to which the appliance belongs replaces the name and description you provided in step 4, since the appliance can only belong to one cluster. The Cluster members screen is displayed, showing the members of the appliance's cluster.

10 To add a new member to the cluster, click **Add** to display the Connect to cluster member dialog box.

   You can also delete an existing member from the cluster by selecting the IP address and clicking **Delete**.

11 Enter the IP address, password, and management port number of another appliance and click **OK**.

   The new member's IP address is added to the Cluster members screen and your connection is verified.

12 Repeat steps 10 and 11 for each cluster member to be added.

13 When all the cluster members have been added, click **Next** to display the Define primary subnet and virtual IP address screen.

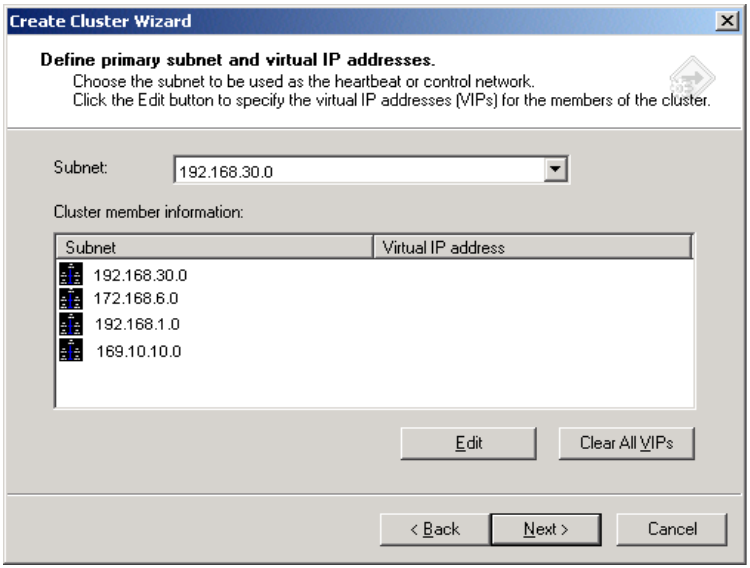


Figure 11-5 Define primary subnet and virtual IP addresses page

14 Use the **Subnet** list to choose a subnet to be used as the controlling network. The inside network is selected by default.

15 Select a Subnet from the Cluster member information list and click **Edit** to display the VIP Addresses dialog box.

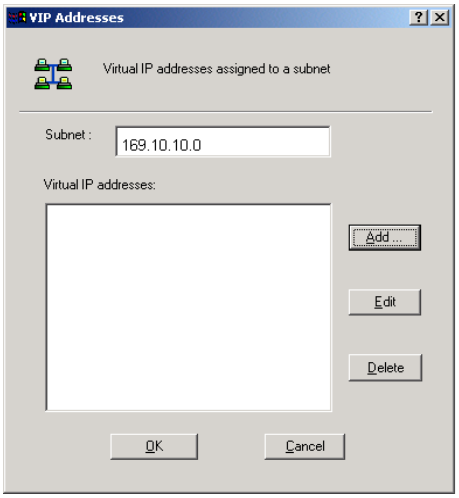


Figure 11-6 VIP Addresses dialog box

16 Click **Add** to display the Add a Virtual IP Address dialog box.

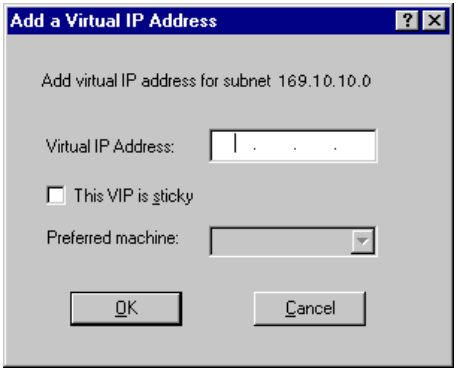


Figure 11-7 Add a Virtual IP Address dialog box

This dialog box allows you to provide a virtual IP address (VIP) for the cluster member. This IP address is used to represent the identity of the cluster to outside machines and routers.

Note: You must assign at least one VIP address to each subnet of the cluster.

---

17 The VIP address can be assigned in three different ways, depending on your cluster requirements.

- Enter a Virtual IP Address for the cluster member without doing anything else in this dialog box.

  This creates a normal VIP that is free to participate in load balancing. It does not have any type of "stickiness" associated with it.

- Enter a Virtual IP Address for the cluster member and check the **This VIP is sticky** check box.

  This creates a sticky VIP that will stay on the node it is assigned to as long as that node is healthy. If the node goes down, the VIP is transferred to another node in the cluster. When the original node comes back up, the VIP stays with the node that it transferred to.

- Enter a Virtual IP Address for the cluster member, check the **This VIP is sticky** check box, and choose the IP address of a preferred appliance for the VIP to be associated with.

  This creates a sticky VIP that has a preference for the IP address you select. It will stay with the node it is assigned to as long as that node is healthy. If the node goes down, the VIP is transferred to another node in the cluster. When the node the VIP was originally assigned to is back up, the VIP returns to it.

Note: With symmetric routing turned on, sticky VIPs do not effect the node that actually owns the connections, simply where the traffic is first seen. You can implement your own symmetric routing by having sticky VIPs bound to particular machines and then distribute them in a load balanced way. Then turn asymmetric routing on and the incident node is the owner node for the traffic.

---

18 Click **OK** to process the Add a Virtual IP Address dialog box, then click **OK** again to close the VIP Addresses dialog box.

The VIPs you have assigned are shown in the Cluster member information list.

19 Repeat steps 15 through 18 for each subnet, then click **Next** to display the final screen of the Cluster Wizard.

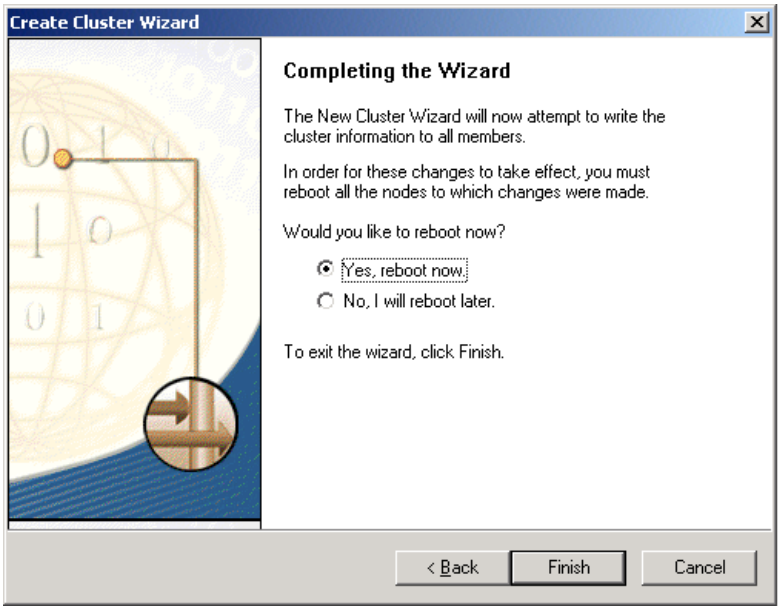

Create Cluster Wizard
Completing the Wizard
The New Cluster Wizard will now attempt to write the cluster information to all members.
In order for these changes to take effect, you must reboot all the nodes to which changes were made.
Would you like to reboot now?
Yes, reboot now.
No, I will reboot later.
To exit the wizard, click Finish.
< Back
Finish
Cancel

Figure 11-8 Completing the Wizard page

20 Decide whether to reboot the cluster members now or later.

If you choose **Yes, reboot now**, all appliances in the cluster will be rebooted.

21 Click **Finish** to complete the wizard.

You are returned to the SRMC. The newly created cluster appears as an icon in the left pane. By expanding it, you can see all the members of the cluster.

You may want to delete the previous individual appliances that are now members of the cluster.

The **Integrated Software HA/LB** cluster the members of the cluster will start to work as an integrated software HA/LB cluster after rebooting.

Creating a cluster for appliance file propagation or hardware HA/LB

Clusters can be used to propagate configuration information such as rules, users, and entity definitions from one appliance to other appliances. The following procedure does not involve any HA/LB configuration.

Before you run the Cluster Wizard, make sure that the IP addresses and passwords of all the appliances you want to add to the cluster have been defined on all the Symantec Gateway Security appliances that will be added to the cluster.

To create a cluster of appliances for propagation of configuration files or hardware HA/LB

1. Click the **Symantec Raptor Management Console** icon to display the Getting Connected taskpad.
2. Click the **New Cluster** icon to display the Cluster Create Wizard.
3. Click **Next** to display the Create a new cluster screen as shown in Figure 11-2.
4. Enter a name and description for the cluster.
5. Click one of the following radio buttons:
   - To create a hardware HA/LB cluster, click **Hardware HA/LB**
   - To create a cluster for propagation of configuration files only, click **Other replication**.
6. Click **Next** to display the Cluster members screen as shown in Figure 11-3.
7. To add the first member to the cluster, click **Add** to display the Connect to cluster member dialog box, as shown in Figure 11-4.
8. Enter the IP address, password and management port number of the first cluster member.

Note: The **Obtain read/write access upon connecting** check box is grayed out and can not be edited. When the Cluster Wizard attempts to connect you to an appliance, you must have read/write access to add the appliance to the cluster.

---

9. Click **OK**.

   The Cluster wizard attempts to connect to the appliance.

   - If this is the first time this appliance is being added to a cluster, the **Cluster members** screen is re-displayed, showing the IP address of the appliance and verifying that you are connected.

     If the appliance is already a member of a cluster, a message asks if you want to read the existing information for the appliance.
   - If you click **Yes**, the name and description of the cluster to which the appliance belongs replaces the name and description you provided in Step 4, since the appliance can only belong to one cluster. The **Cluster members** screen is displayed, showing the members of the appliance's cluster.
10. To add a new member to the cluster, click **Add** to display the **Connect to cluster member** dialog box.

    You can also delete an existing member from the cluster by selecting the IP address and clicking **Delete**.

11 Enter the IP address, password, and management port of another appliance and click **OK**.

   The new member's IP address is added to the Cluster members screen and your connection is verified.

12 Repeat Steps 10 and 11 for each cluster member to be added.

13 When all the cluster members have been added, click **Next** to display the final screen of the Cluster Wizard.

14 Click **Finish** to complete the wizard.

   You are returned to the SRMC. The newly created cluster appears as an icon in the left pane. By expanding it, you can see the members of the cluster.

If you created a **Hardware HA/LB** cluster the cluster is ready to be connected a Radware FireProof™ device. Radware's FireProof™ is an intelligent traffic management device for multiple firewalls and Virtual Private Network (VPN) devices. See www.radware.com for more information.

Verifying a cluster

Verifying a cluster allows you to be sure that the cluster configuration information is identical on all cluster members. For example, if a machine was down when you last made changes, it may not have the latest cluster configuration information.

If your cluster members do not have identical cluster information, the Verify Cluster wizard allows you to choose a cluster member so that its configuration can be copied to all other members.

To verify a cluster

1 Connect to a member of the cluster you want to verify.

2 In the left pane, right click on the cluster name.

3 Choose **All Tasks** > **Verify Cluster** to display the Verify Cluster Wizard.

4 Click **Next.**

5 If there are cluster members that are not connected, the Connect to cluster members screen is displayed. Enter the password for the system whose IP address is displayed and click **Next**.

6 Repeat step 5 until all members are connected, at which point one of the following screens is displayed:

   - If the **Completing the Wizard** screen displays, saying that the configuration is in a consistent state, the verification process has been completed successfully. Click Finish to close the Verify Cluster Wizard.

- If the **Cluster configuration not in sync** screen is displayed, continue at step 7.

7 Choose a cluster member from the list and click **Next**.

If the member you chose is valid, the **Verify cluster** screen is displayed, showing the cluster information of the member.

a Click **Next**. The **Cluster configuration chosen** screen is displayed. This screen is read only.

b Click **Next** to display the **Completing the Wizard** screen.

c Click **Finish** to write the configuration of the selected cluster member to all other members.

If the member you chose is not valid, a message box tells you that the member's information is incorrect and cannot be restored.

a Click **OK** to clear the message and return to the Cluster configuration not in sync screen. The invalid cluster is marked.

b Choose another cluster member from which the cluster information will be copied, and click **Next**.

c Repeat until the Cluster configuration chosen screen is displayed. This screen is read only.

d Click **Next** to display the **Completing the Wizard** screen.

e Click **Finish** to write the configuration of the selected cluster member to all other members.

Modifying a cluster

There are two reasons to modify a cluster:

- To make changes to the cluster configuration information and copy those changes to all members of the cluster.
- To enable or disable a cluster member prior to using the Propagate option. Propagate copies the appliance configuration files from a selected appliance's sg directory to all enabled members of that appliance's cluster.

To access the Modify Cluster Wizard, you must be connected to at least one cluster member.

To modify a cluster

1 In the left pane, right click the cluster name.

2 Choose **All Tasks>Modify Cluster** to display the Modify Cluster Wizard.

3 Click **Next** to display the **Modifying a cluster** screen.

You can change the cluster name and description. By default, the **Automatically connect to all disconnected cluster members** check box is checked. The modifications you make will only be copied to members that are connected. Uncheck this check box if you do not want to connect to all cluster members.

Note: Symantec recommends that you connect to all cluster members when modifying a cluster so that the modifications you make are distributed to all members.

---

4 Click **Next**.

- If the option to automatically connect was checked, the wizard connects to all cluster members, and then displays the Cluster members screen.
- If the option to automatically connect was not checked on the previous screen, the Connect to cluster members screen is displayed.
- If you want to connect the cluster member whose IP address is shown, enter the password and, if necessary, change the management port, then click **Next** to connect. Repeat for all cluster members to which you want to connect.
- If you do not want to connect to a member, select the **Ignore this member** check box and click **Next**.

Note: Modified cluster information is **not** copied to members which are ignored.

After you have been given the chance to connect to all cluster members, the wizard displays the Cluster members screen.

5 On the Cluster members screen, you can:

- Click **Add** to add a new cluster member.
- Click **Delete** to delete a member of the cluster.
- Uncheck the check box to the left of a cluster member's icon to disable the cluster member. This causes the cluster member to be ignored when appliance configuration files are propagated.
- If a cluster member has been disabled, select the check box to enable the cluster member to participate in the propagation of appliance configuration files.

6 When you have completed all changes to the cluster member screen, click **Next**.

- If the cluster is not an HA/LB cluster, the final screen of the wizard is displayed. Go to Step 13.
- If the cluster is an HA/LB cluster, the **Define primary subnet and virtual IP addresses** screen is displayed. Complete steps 7 through 12.

7 To change the subnet that is selected to act as the heartbeat network, click **Clear All VIPs**, then use the **Subnet** drop down list to select a different subnet. You must then create virtual IP addresses (VIPs) for all subnets.

8 To change or create a VIP, select a subnet in the Cluster member information list and click **Edit** to display the **VIP Addresses** dialog box.

9 The VIP Addresses dialog box provides the following options:

- Select an existing VIP and click **Edit** to edit it or **Delete** to delete it.
- To add a new VIP, click **Add**.

Clicking **Add** or **Edit** displays the Add a Virtual IP Address dialog box.

10 Complete the Add a Virtual IP Address dialog box as follows:

Note: Symantec recommends that the VIP address is higher than the physical IP address of the nodes in the cluster.

- Enter a Virtual IP Address for the cluster member without doing anything else in this dialog box.
- This creates a normal VIP that is free to participate in load balancing. It does not have any sort of stickiness associated with it.
- Enter a Virtual IP Address for the cluster member and check the **This VIP is sticky** check box.
- This creates a sticky VIP that will stay on its current node as long as that node is healthy. If the node goes down, the VIP is transferred to another node in the cluster. When the original node comes back up, the VIP stays with the node that it transferred to.
- Enter a Virtual IP Address for the cluster member, check the **This VIP is sticky** check box, and choose an IP address for the VIP association.

  This creates a sticky VIP that has a preference for the IP address you select. It will stay with the node it is assigned to as long as that node is healthy. If the node goes down, the VIP is transferred to another node in the cluster. When the original node is back up, the VIP returns to it.

Note: With symmetric routing turned on, sticky VIPs do not effect the node that actually owns the connections, simply where the traffic is first seen. You can implement your own symmetric routing by having sticky VIPs bound to particular machines and then distribute them in a load balanced way. Then, turn asymmetric routing on and the incident node is the owner node for the traffic.

11 Click **OK** to process the Add a Virtual IP Address dialog box, then click **OK** again to close the VIP Addresses dialog box.

12 When all VIP addresses have been modified, click **Next** to display the final wizard screen.

If the cluster you are modifying is a software HA/LB cluster, you will be prompted to reboot so that the modifications you have made can be registered.

13 On the **Completing the Wizard** screen, click **Finish** to write the modified cluster configuration to all files in the cluster.

Deleting a cluster

To access the Delete Cluster Wizard, you must be connected to at least one cluster member.

Note: The process of deleting a cluster does not delete any appliances. It simply removes the configuration information that associates them into a cluster.

To delete a cluster

1 In the left pane, right click the cluster name.

2 Choose **All Tasks>Delete Cluster** to display the Delete Cluster Wizard.

3 Click **Next** to display the Deleting a cluster screen.

By default, the **Automatically connect to all disconnected cluster members** check box is checked. The cluster can only be deleted if all members are connected so that the cluster information can be deleted from them.

4 Click **Next**.

- If the option to automatically connect was checked, the wizard connects to all cluster members, and then displays the Completing the Wizard screen.

- If the option to automatically connect was not checked on the previous screen, the **Connect to cluster members** screen is displayed to allow you to connect.

5 Enter the password and, if necessary, change the management port for the cluster member whose IP address is shown.

6 Click **Next** to connect.

When all members of the cluster are connected, the Completing the Wizard screen is displayed.

7 Click **Finish** to delete the cluster configuration from all members.

If you are deleting a software HA/LB cluster, you will be prompted to reboot so that cluster information can be removed from the registry.

Viewing Cluster Properties

Note: Although you can view the properties of a cluster, the details you see are read only. If you want to make changes, you must do so by using the Modify Cluster wizard. For more information, see **Modifying a cluster**.

To view the properties of a cluster

1 Expand the cluster's folder in the left pane.

2 Connect to a member of the cluster.

You must be connected because the cluster configuration information is stored on the cluster members.

3 Right click on the cluster's icon and choose **Properties**. The cluster's Properties pages are displayed.

The **General** tab shows the name and description of the cluster, and tells you what type of cluster it is.

The Member field gives the IP address of the connected member.

4 Click the **Members** tab.

This tab lists the members of the cluster and indicates whether they are enabled for propagation.

5 If the cluster is an Integrated Software High Availability and Load Balancing (HA/LB) cluster, click the **VIPS** tab to view information about the Virtual IP (VIP) addresses in use by the cluster.

The virtual IP addresses list shows the cluster subnets and the VIP addresses that are assigned to them.

To see details about a specific subnet, double click the subnet to display the VIP addresses dialog box.

To see details about a specific VIP address, double click the address.

Click **OK** to close each additional dialog box you display.

6 Click **OK** to close the cluster's Properties page.

Propagating appliance configuration files

When you secure your network using multiple appliances, it is important to have consistency between appliance configurations. You want to be sure that entities are defined in the same way on all systems, and that the same authorization rules and authentication procedures are in place.

Propagation allows you to configure one appliance and copy the configuration information to other appliances that are grouped in a cluster.

Among the files that are copied to the other appliances is the host file from the source machine. The source host file overwrites the target host files, rather than merging with them.

Do the following before running Propagate, so that DNS entries are not overwritten

1 On the appliance from which you will propagate, use the DNS Records Properties page to create an entry in the Hosts file for each of the other appliances in the cluster.

2 Create entities for the all configured interfaces of all the nodes in the cluster.

To propagate appliance configuration files

1 Associate the appliances protecting your network into a cluster. See **Creating a cluster for appliance file propagation or hardware HA/LB on page 222**.

2 Make your changes to a selected appliance system in the cluster.

3 Decide whether to propagate appliance configuration files to all members of the cluster, or to disable some cluster members so that their configuration files remain unchanged. See also **Modifying a cluster on page 225**.

Note: Symantec recommends that you propagate to all cluster members.

---

4 In the left pane, click on the icon of the appliance where changes have been made.

5 Right click and choose **All Tasks**>**Propagate**, or display the Action menu and choose **All Tasks**>**Propagate**.

6 A message box asks if you are sure you want to propagate. Click **Yes**.

The Result of configuration propagation status box is displayed.

For each appliance in the cluster, the appliance service is temporarily stopped so that the configuration files can be copied to the appliances.

The status box displays the following messages as the backup file from the source appliance is restored:

```
Processing  Wait...

Updating SRMC view Wait...

Restarting Services Wait...

Propagation Done
```

7 When the configuration has been propagated to all enabled members of the cluster, click **OK** to close the status box.

HA/LB Implementation

The Symantec Gateway Security appliance is a critical component of network security. A single appliance configuration (a network without HA/LB) may not be appropriate for all situations for the following reasons:

- Single point of failure
- Possible bottleneck

As a single point of failure, if the appliance is down, your external users no longer have access to internal resources, and your internal users are cut off from external networks. Although the network is still secure, it is off-line until the appliance is restored to service.

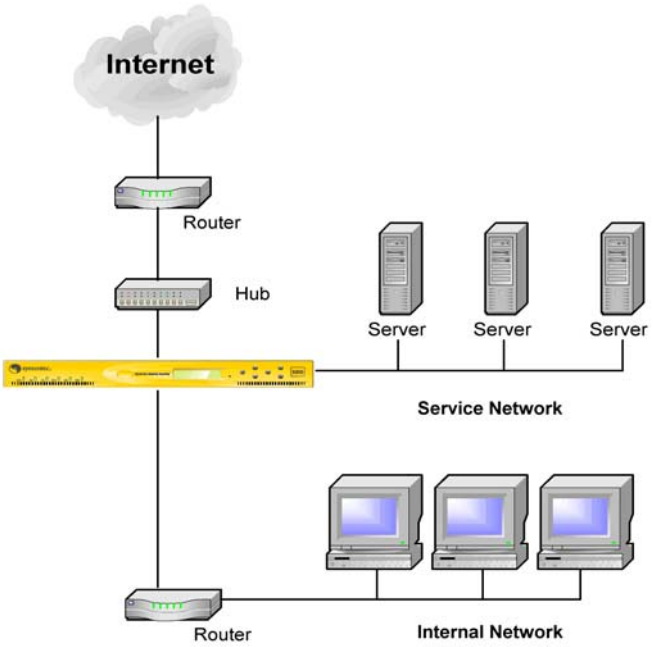


Figure 11-9 Non HA/LB network

One solution is to add additional appliances to your company network. Multiple appliances can be configured to act as if they were one gateway. This is referred to as a cluster. If one member of a cluster has a failure the others will continue to operate and pick up the load (network traffic) of the failed appliance without any interruption of service to the users of the network.

The following example depicts a three appliance software HA/LB cluster. The first step in creating this cluster is to physically setup and configure the appliances on the network. Internal and external interfaces on each appliance must be configured properly, and the networks that each appliance talks to must also be configured.

The second step is the setup of virtual IP address (VIPs) on the network. See **Cluster members screen on page 235**.

Three appliance cluster example

In this example, each of the three Symantec Gateway Security appliances uses all four of its network ports (located on the back panel of the appliance), as shown in **Figure 11-10**, to connect to the networks shown in **Figure 11-11**.

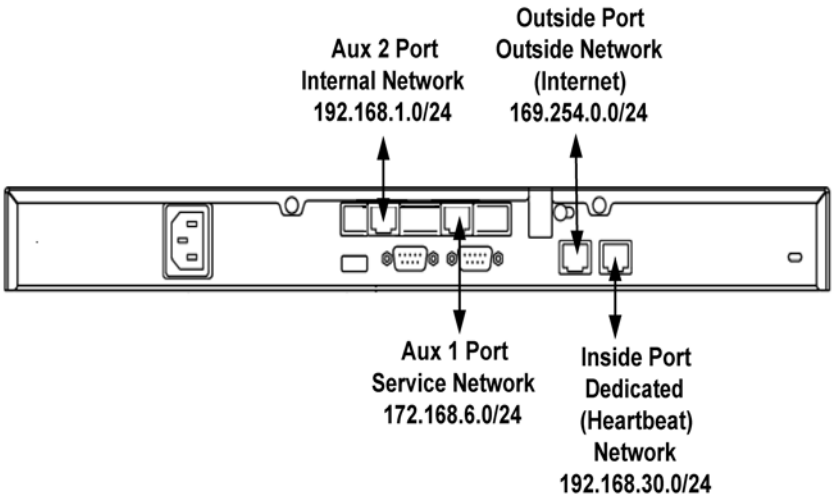


Figure 11-10 Symantec Gateway Security appliance back panel

Each of the three appliances is configured and connected to the network in the same way. Even if two of the appliances fail, the third appliance will pick up the load. The three internal networks will still be secure and online, although with diminished throughput capacity because one appliance is bearing the full network load.

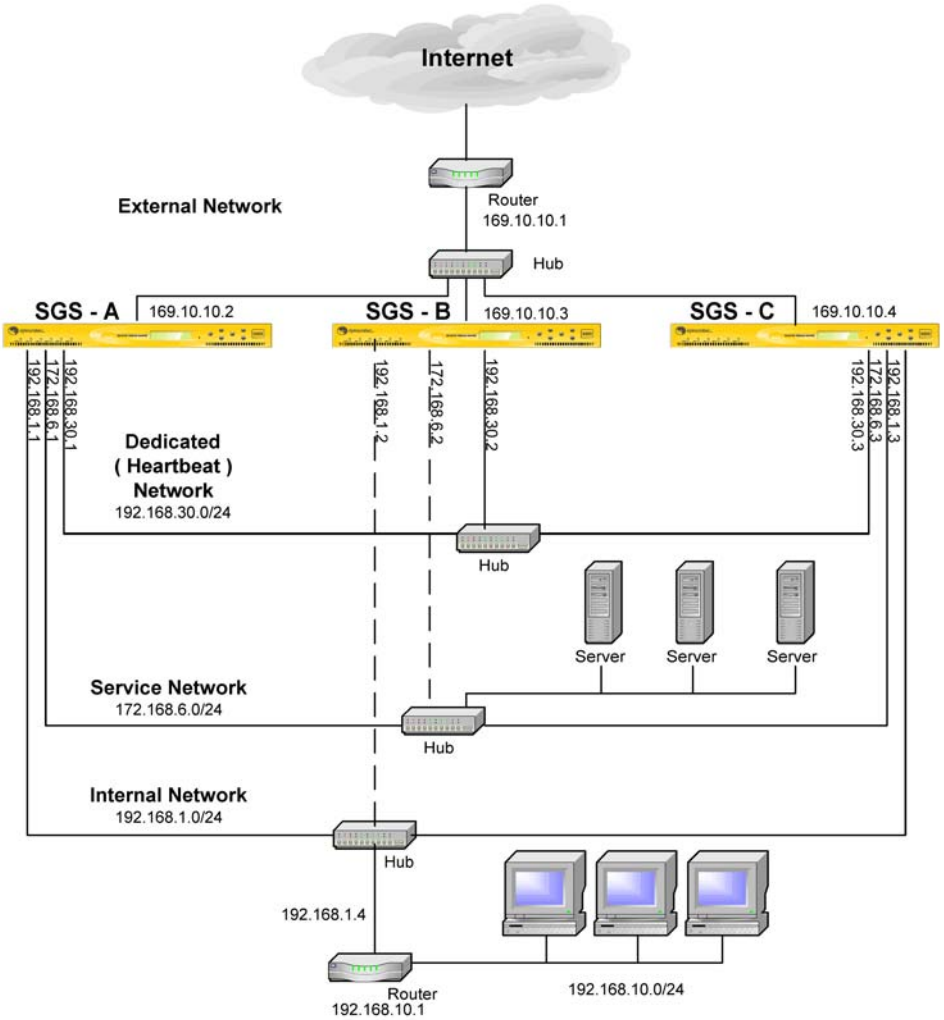


Figure 11-11 Three appliance cluster network diagram

Figure 11-11 is a three appliance HA/LB network diagram that shows a typical Symantec Gateway Security cluster implementation. Our clustered network consists of the following components:

- **External network:** The external network is the 169.10.10.0/24 network. This network connects to the Internet through our router (169.10.10.1).

- **Dedicated network:** The dedicated network is the 192.168.30.0/24. It is used as the heartbeat or control network. Each appliance in the cluster uses the heartbeat network to exchange state information about the cluster.
- **Service network:** Our service network is the 172.168.6.0/24 network. A service network could have Web, SMTP and FTP servers. This network could contain many machines and subnets.
- **Internal network:** Our internal network is the 192.168.1.0/24 network. This network could contain many machines and subnets.

Note: A heartbeat network does not have to be a dedicated network dedicated to only heartbeat communications as shown in this example. Heartbeat communications can run on any internal network with other traffic and subnets.

To create this cluster, use the Create Cluster Wizard and follow the steps in Creating a cluster for software high availability/load balancing on page 215. When you get to the Cluster members screen you would add cluster members using their IP Addresses as shown in Figure 11-12.

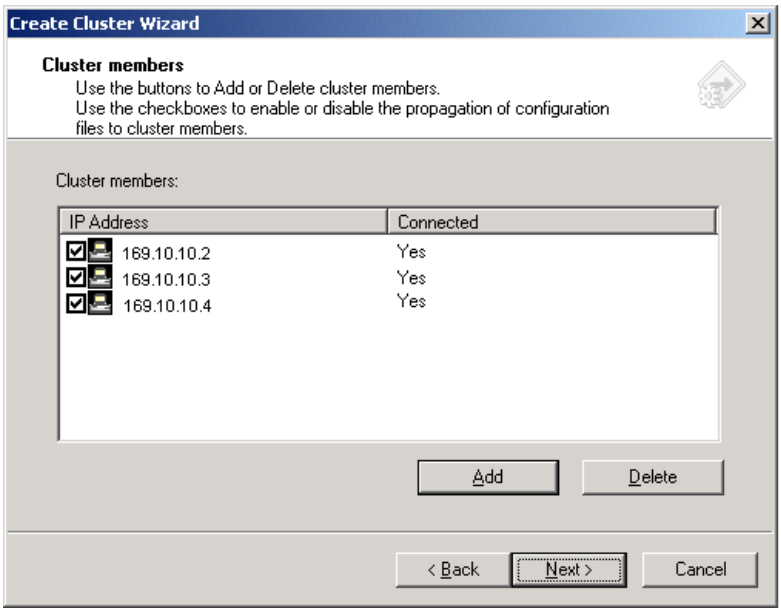


Figure 11-12 Cluster members screen

Setting Up VIPs

Setting up virtual IP addresses (VIPs) for this cluster is the next step. Each machine in the cluster shares the same virtual IP address for a given subnet, and is viewed as a potential candidate to receive packets. If one appliance fails, another appliance handles any new requests, providing continued connectivity to your network. **Figure 11-13** shows our example with VIPs.

Because the VIP is assigned to a subnet, all of the machines in the cluster on the subnet are viewed as a single IP address. With load balancing configured, this allows the cluster to spread the connections more evenly over several different appliances, instead of always sending requests to one appliance.

Note: The VIP should be assigned using an IP address higher than any of the nodes supporting that VIP.

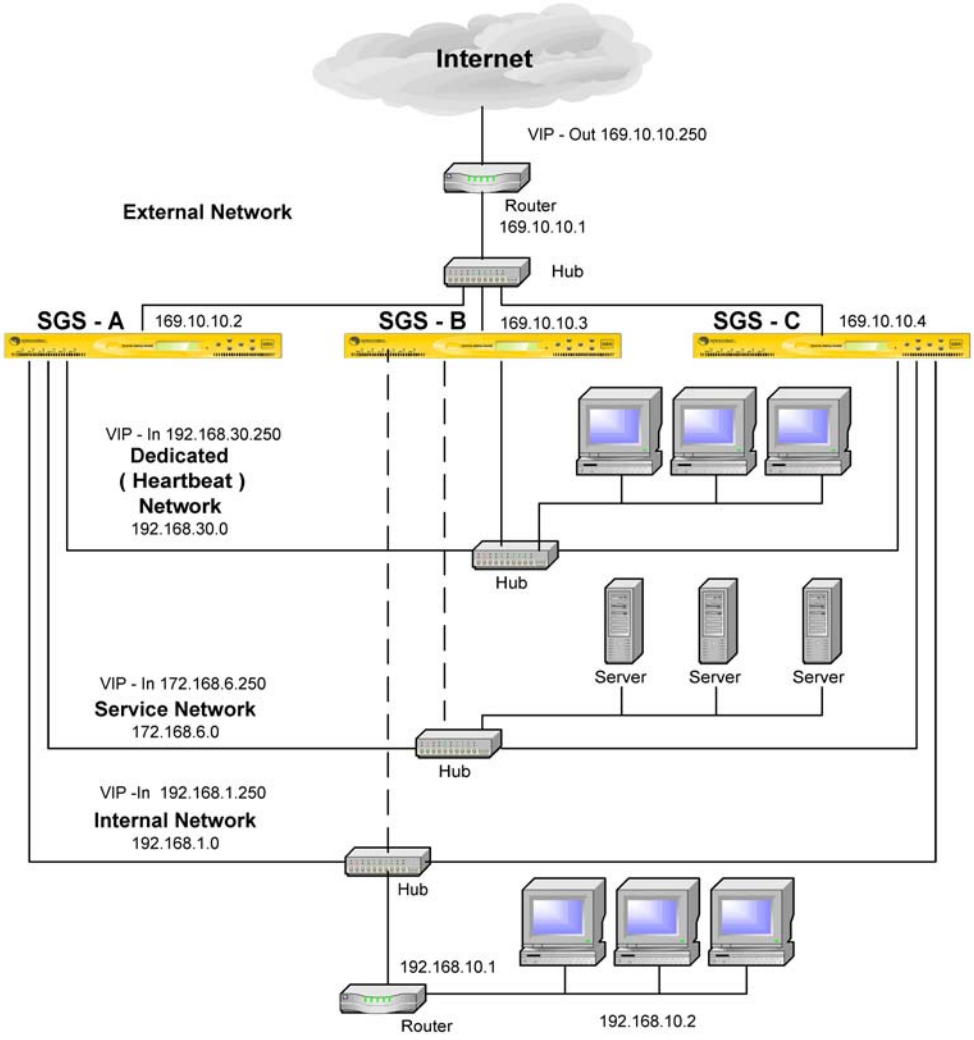


Figure 11-13 HA/LB cluster with VIPs

The next step is to modify the routing tables on each of the each of the machines and servers on each of the networks. All machines and servers must now point to the VIPs instead of the real IP addresses for HA/LB to work properly. If the machines and servers continued to point to the real IP addresses of the appliances, and one of the appliances failed, all of the machines and servers

pointing to that security gateway would be cut off from the network. The following table shows the VIP settings for our cluster network.

Table 11-1 VIP addresses

Network Address	VIP Address	Network Type
169.10.10.0/24	169.10.10.250	Outside - Internet
192.168.30.0/24	192.168.30.250	Dedicated - Heartbeat
172.168.6.0/24	172.168.6.250	Service
192.168.1.0/24	192.168.1.250	Internal

We set the default gateway of our dedicated (heartbeat) network machines to VIP 192.168.30.250. We set the default gateway of our internal network machines (everything on the 192.168.1.0/24 network) to VIP (192.168.1.250). We also change the default gateway of the interface on the servers residing on our service network to point to VIP (172.168.6.250). Each of these are different networks and therefore we need to have a different VIP configured for each one.

DNS resolvers must be configured to point to the individual IP addresses of the appliances, not the VIP addresses.

Finally, we configure a static route on the 169.10.10.1 router (outside network - internet) that says that all traffic destined for the 169.10.10.0/24 network should go through the VIP 169.10.10.250.

To configure VIPS, use the Create Cluster Wizard and follow the steps in **Creating a cluster for software high availability/load balancing on page 215**. When you get to the Define primary subnet and virtual IP addresses screen, you would assign a subnet to be the heartbeat network and assign VIP addresses to cluster members as shown in **Figure 11-14**.

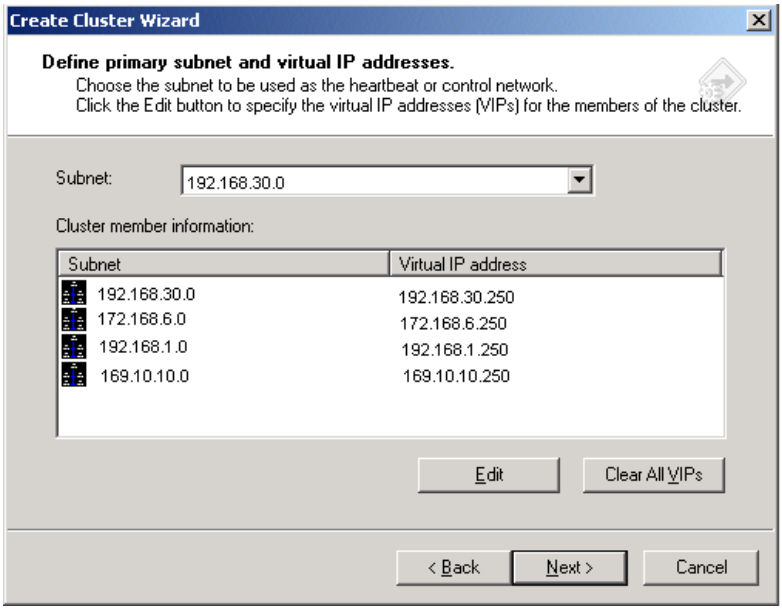


Figure 11-14 Define primary subnet and virtual IP address screen

We use the VIP addresses as reference points to previous definitions that would otherwise use a physical address. Doing this removes any single point of failure. In our example, three appliances are virtually known by one VIP address and seem to be one appliance. They still have different physical addresses, but everybody addresses each appliance by its virtual IP address. Multiple machines in the cluster can have the same virtual IP address, so if one fails, another can take its place and no additional routing needs to take place.

The one SRMC exception to addressing the Symantec Gateway Security appliances by their VIP address is connecting to appliances and managing them. You cannot use the VIP address in the SRMC because you cannot be guaranteed of connecting to the specific appliance you desire. Any appliance on your network could be the active one at any given time. Therefore, all SRMC connections must be directed to the real IP address of the security gateway you wish to manage.

HA/LB terms

Incident node

Only one machine has control of the VIP at any given time. This machine is referred to as the incident node. The incident node receives ownership of the VIP, and all communication requests directed to the VIP are handled by the incident node.

When a communication request comes in to the incident node, the incident node is responsible for:

- Serving the request
- Passing on the initial request to another node in the cluster
- Passing on the request to the node that is currently serving the connection

If a failure occurs on the incident node, another node in the cluster becomes the incident node, claims ownership of the VIP, and assumes responsibility for all new connection requests entering the cluster.

Heartbeat network

An internal network that acts as the heartbeat or control network. The heartbeat network is used by each appliance in the cluster to exchange state information about the cluster. The heartbeat network does not have to be dedicated to heartbeat communications only, however this a preferred configuration.

Sticky node

A node in the cluster can be designated as a sticky node. If a node is marked as sticky, and requests are currently being sent to it, requests will continue to be sent to this node until this node is no longer available (due to a failure). If one node gives up the sticky bit, it will jump to the next node picked to be the incident node, and remain there until that node is no longer available, even if the first node comes back up.

Preferred node

A node in the cluster can also be designated as a preferred node. A preferred node can be thought of as a persistent sticky node. By specifying that a node is preferred, communication requests will always be sent to this machine when it is available. If this machine is unavailable, another machine on the cluster will become the incident node, but will not be marked as the preferred node. If the

first machine comes back up, communication requests will revert back to the first machine until it is no longer available.

Symmetric routing

Symmetric routing assures that any return packets for a connection go back out through the same security gateway.

Asymmetric routing

Asymmetric routing is the default mode for the appliance until the Cluster Wizard is run for the first time. Asymmetric routing allows a return packet for a connection to go back out through any security gateway in the cluster. Asymmetric routing provides for better network performance, especially if the incident node is busy. State information must be maintained between all of the nodes in the cluster for asymmetric routing to work properly.

Appendix A

Important safeguards

For your protection, please read all these instructions regarding your Symantec Gateway Security appliance.

1. Read Instructions

   Read and understand all the safety and operating instructions before operating the appliance.

2. Ventilation

   The Symantec Gateway Security appliance's vents (on the front) and the fan opening(s) on the back panel are provided for ventilation and reliable operation of the product and to protect it from overheating. These openings must not be blocked or covered. This product should not be placed in a built-in installation unless proper ventilation is provided.

3. Lithium Battery

   The lithium battery on the system board provides power for the real-time clock and CMOS RAM. The battery has an estimated useful life expectancy of 5 to 10 years.

4. Power Cord

Caution: The power-supply cord is used as the main disconnect device. Ensure that the socket outlet is located or installed near the equipment and is easily accessible.

Caution: Français: Le cordon d'alimentation sert d'interrupteur général. La prise de courant doit être située or installée à proximité du matérial et offrir un accès facile.

Caution: Deutsch: Zur sicheren Trennung des Gerätes vom Netz ist der Netzstecker zu ziehen. Vergewissern Sie sich, daß die Steckdose leicht zugänglich ist.

5 Electrical Shock

To reduce the risk of electrical shock, do not disassemble this product. Return it to Symantec when service or repair work is required. Opening or removing covers may expose you to dangerous voltage or other risks. Incorrect reassembly can cause electric shock when this product is subsequently used.

Note: Opening the cover will void your warranty!

6 Operating the unit in an equipment rack

If you plan to install the Symantec Gateway Security appliance in an equipment rack, use these precautions:

- Ensure the ambient temperature around the appliance (which may be higher than the room temperature) is within the limits specified in **Appliance models and specifications on page 13**.
- Ensure there is sufficient air flow around the unit.
- Ensure electrical circuits are not overloaded; consider the nameplate ratings of all the connected equipment and ensure you have overcurrent protection.
- Ensure the equipment is properly grounded, particularly any equipment connected to a power strip.
- Do not place any objects on top of the appliance.

Appendix B

IDS and antivirus scanning log messages

This appendix describes:

- Messages that are sent to the system log file as a result of IDS alerts
- Messages sent from the Antivirus scan server as a result of antivirus scanning

  Antivirus scanning is associated with two types of messages:
  - Customizable messages that are sent to users when viruses are detected
  - System logfile messages

IDS Messages

IDS notifications are generated for IDS messages only and System notifications are generated for system (non-IDS) messages. All log messages/events that say they are an "IDS Alert" are used for generating IDS notifications and not used when generating System notifications. All log messages/events that do not say they are an "IDS Alert" are used for generating system notifications and are not used when generating IDS notifications.

IDS messages may be of two types:

- Informational messages (message number 100)
- IDS alerts (message numbers 525, 550, 575)

Both types of messages are recorded in the logfile that the system collects on all connections and connection attempts to the gateway.

To view the system logfile messages

1. Expand the **Monitoring Controls** node.
2. Expand the **Logfiles** icon.
3. Click the month of the log file you want to view.

   A list of logfiles is displayed in the right pane.

   The logfiles are named by date, with the extension in the format yyyymmdd.

   For example: logfile.20010918
4. Double click the logfile you want to view to display the events it contains in the right pane.

The format of messages in the system logfile is provided in Table B-1.

Table B-1 System Logfile Message Format

Event Type	Lists the type of message being logged (information, warning, etc.)
System Name	Lists the system name where the logged event took place
Component	Lists the daemon or action that is being logged
PID	Lists the Process ID number of the logged event
Timestamp	The time the attack was logged on the appliance

Table B-1 System Logfile Message Format

Message Number	Lists the log number of the event or action
Message Text	Lists further detail about the log entry

IDS Informational Messages

This section describes IDS informational messages, which have a message number of 100.

The format of IDS informational messages is provided in Table B-2.

Table B-2 IDS informational message formats

Event Type	Information
System Name	System name (as entered in the System tab of the Properties page)
Component	• kernel for module startup and shutdown messages • lograptor for all other messages
PID	a dash (-)
Timestamp	The time the attack was logged on the appliance
Message Number	100
Message Text	See list of messages in Table B-3.

The message text can be any one of the messages listed in Table B-3. An explanation and a description of user action for each message is included in this table.

Table B-3 IDS informational messages

Message	100 IDS Info: IDS kernel module startup
Explanation	The IDS kernel module (ids.o) has been started.
User Action	None.

Table B-3 IDS informational messages

Message	100 IDS Info: IDS kernel module shutdown
Explanation	The IDS kernel module has been shut down.
User Action	None.
Message	100 IDS Info: IDS LiveUpdate: Preparing for IDS LiveUpdate
Explanation	LiveUpdate process starting.
User Action	None.
Message	100 IDS Info: IDS LiveUpdate: LiveUpdate failed
Explanation	There is a problem downloading the files from the LiveUpdate server. This may occur if one or more of the following occurs: • The appliance cannot connect to the LiveUpdate server. • The files cannot be located on the LiveUpdate server. • The files downloaded from the LiveUpdate server cannot be placed in the existing directory structure. • The LiveUpdate file is corrupted.
User Action	Perform the following: • Ensure that the server specified in the LiveUpdate Properties window is valid. • Either click Run LiveUpdate Now in the LiveUpdate Properties window, or allow LiveUpdate to run as scheduled to update the files on the appliance.
Message	100 IDS Info: IDS LiveUpdate: IDS LiveUpdate process completed, failed merge

Table B-3 IDS informational messages

Explanation	The downloaded sigs.conf file cannot be merged with the existing sigs.conf file. This may occur if one or more of the following occurs: • There is a mismatch in the signature order in the downloaded file. • There is a mismatch in the field count for one or more signatures in the downloaded file.
User Action	Run LiveUpdate again.
Message	100 IDS Info: IDS LiveUpdate: IDS LiveUpdate process completed and new module installed
Explanation	All files were downloaded and installed successfully.
User Action	None.
Message	100 IDS Info: IDS LiveUpdate: IDS LiveUpdate process completed, module load failed
Explanation	The downloaded IDS kernel module (ids.o) file cannot replace the existing file; no module installed.
User Action	Contact Customer Support.
Message	100 IDS Info: IDS LiveUpdate: IDS LiveUpdate process completed, files out of sync
Explanation	The version numbers of the downloaded IDS kernel module (ids.o) and the sigs.conf files do not match.
User Action	Contact Customer Support.
Message	100 IDS Info: IDS LiveUpdate: IDS LiveUpdate process completed with no change
Explanation	The same or newer version of the files is already installed; there is no need to update.
User Action	None.

Table B-3 IDS informational messages

Message	100 IDS Info:IDS LiveUpdate: Schedule set failed
Explanation	The scheduled update was not set successfully in the system schedule.
User Action	Re-enter the schedule event in the LiveUpdate Properties window.
Message	100 IDS Info: IDS LiveUpdate: Schedule set successfully
Explanation	The scheduled update is set successfully in the system schedule.
User Action	None.
Message	100 IDS Info: IDS LiveUpdate: Schedule clear failed
Explanation	The scheduled update was not removed successfully from the system schedule.
User Action	Ensure that the Enable Schedule checkbox is not checked in the LiveUpdate Properties window. If the problem persists, contact your administrator to manually remove the entry in the system schedule.
Message	100 IDS Info: IDS LiveUpdate: Schedule cleared successfully
Explanation	The scheduled update was removed successfully from the system schedule.
User Action	None.
Message	100 IDS Info: IDS LiveUpdate: LiveUpdate Now Failed

Table B-3 IDS informational messages

Explanation	There is a problem downloading the files from the LiveUpdate server when Run LiveUpdate Now is clicked in the LiveUpdate Properties window. This may occur if one or more of the following occurs: • The appliance cannot connect to the LiveUpdate server. • The files cannot be located on the LiveUpdate server. • The files downloaded from the LiveUpdate server cannot be placed in the existing directory structure. • The LiveUpdate file is corrupted.
User Action	Perform the following: • Ensure that the server specified in the LiveUpdate Properties window is valid. • Click Run LiveUpdate Now in the LiveUpdate Properties window.
Message	100 IDS Info: IDS Signature Config: Update file does not exist
Explanation	The updated sigs.conf file is not found on the Symantec Gateway Security appliance.
User Action	Re-enter the signature configuration changes in the SRMC GUI, and click Save and reconfigure.
Message	100 IDS Info: IDS Signature Config: IDS Signature Config: version check failed
Explanation	The version of sigs.conf attempted to be written to the Symantec Gateway Security appliance is different from the version currently on the appliance. Signature configuration changes are not saved on the appliance.
User Action	Re-enter the signature configuration changes in the SRMC GUI, and click Save and reconfigure.
Message	100 IDS Info: IDS Signature Config: IDS Signature Config: signature order check failed.

Table B-3 IDS informational messages

Explanation	The order of the signatures in sigs.conf attempted to be written to the Symantec Gateway Security appliance is different from the file currently on the appliance. Signature configuration changes are not saved on the appliance.
User Action	Re-enter the signature configuration changes in the SRMC GUI, and click Save and reconfigure.

Message	100 IDS Info: IDS Signature Config: IDS Signature Config: field count check failed.
Explanation	At least one field for one or more signatures in sigs.conf attempted to be written to the Symantec Gateway Security appliance is different from the file currently on the appliance. Signature configuration changes are not saved on the appliance.
User Action	Re-enter the signature configuration changes in the SRMC GUI, and click Save and reconfigure.

IDS Alerts

IDS alerts report attacks when traffic coming through the firewall matches an enabled IDS attack signature.

Log messages that result from IDS alerts can be viewed by using either the logfile viewer or the IDS Alerts viewer.

The following table shows the format of IDS Alerts when viewing in the system logfile window.

Table B-4 IDS Alert formats

Event Type	Alert log message icon, followed by the word Alert
System Name	System name (as entered in the System tab of the Properties page)
Component	kernel
PID	a dash

Table B-4 IDS Alert formats

Timestamp	The time the attack was logged on the appliance
Message Number	525, 550, 575
Message Text	Alert-specific text

To view alerts using the IDS Alerts viewer

1. Expand the **IDS Components** node.
2. Expand the **Monitoring** node.
3. Click the month of the Alerts log you want to view.

   A list of Alerts logs is displayed in the right pane.

   The Alerts logs are named by date, with the extension in the format yyyymmdd.

   For example: Alerts.20010918
4. Double click the Alerts log you want to view.

   The IDS Alerts are displayed in the right pane.

   New log messages appear at the bottom of the window, scrolling up previous log messages. The SRMC automatically updates the view of the current logfile every 15 seconds while the IDS Alerts Viewer is open.
5. For more information about an alert, double click on the alert in the right pane to display help on the specific IDS attack signature that generated the alert.

The following table shows the format of an alerts message in the IDS Alerts viewer.

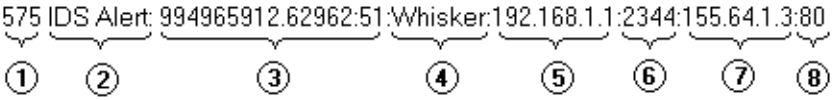
Table B-5 IDS Alerts viewer format

Severity	Severity of the attack
Attack Name	The name of the attack signature
Attack Type	The type of attack
Timestamp	The time the attack was logged on the appliance
Source IP	The source IP address of the attack

Table B-5 IDS Alerts viewer format

Destination IP	The destination IP address of the attack
OS Impacted	The operating systems that can be affected by this attack

The following sample IDS message shows the format of a High severity IDS message in the logfile. The format will be the same for Low and Medium severity messages, except that the message number will be either 525 or 550, respectively.



Where:

1 Message number

2 Indicates IDS Alert

3 Time in seconds and microseconds

4 Attack name

5 Source IP address

6 Source port

7 Destination IP address

8 Destination port

Antivirus scanning messages

There are two types of messages associated with the antivirus scanning:

- Customizable messages that are sent to users when viruses are detected

  For more information about these messages, see **Customizing virus messages on page 197**.
- System logfile messages

This section describes the messages that are sent to the system logfile.

These messages are all 343 Antivirus warnings. The following table lists the messages, describes why each message was generated, and provides a user action where possible.

Table B-6 Antivirus scanning messages

Message	343 Antivirus Warning: The antivirus scan server '%s' cannot be resolved as a hostname
Explanation	The server specified in the config file could not be reached because it is not a valid server name, or a name server could not be reached, or the IP address is invalid.
User Action	Make sure that the server specified is a valid address and that there is an entry in the local DNS server for the address.
Message	343 Antivirus Warning: An invalid value was read for scan options, setting to default: Scan, Repair or Delete
Explanation	There was an error processing a configured value.
User Action	Check the values of the **Scan Options** settings on the Antivirus Scanning tab of the FTPD, HTTPD, and SMTPD proxies to make sure that they are correct. Valid scan option values are: • Scan and Log • Scan and Delete • Scan and Repair or Delete

Table B-6 Antivirus scanning messages

Message	343 Antivirus Warning: Unsupported extension scan option, setting to default: Scan All Files
Explanation	There was an error processing a configured value.
User Action	Check the value of **Which file extensions to scan** settings on the Antivirus Scanning tab of the FTPD, HTTPD, and SMTPD proxies to make sure that they are correct. Valid values are: • All files • Only those in include list • All except those in exclude list

Message	343 Antivirus Warning: Error parsing extension list, restoring default of Scan All Files
Explanation	There is a problem in the list of included or excluded extensions.
User Action	Check the Antivirus Scanning settings for the FTPD, HTTPD, and SMTPD proxies to make sure that they are correct. Make sure that the following rules have been followed: • The extension list is a semicolon delimited list • The only wildcard used is a ? (which means any one character, could be empty) • The extension begins with a period "."

Message	343 Antivirus Warning: Problem with the extension list. Switch to Scan All Files.
Explanation	The SRMC should have sent an extension list to the antivirus scan server but did not.

Table B-6 Antivirus scanning messages

User Action	Check the Antivirus Scanning settings for the FTPD, HTTPD, and SMTPD proxies to make sure that they are correct. Make sure that the following rules have been followed: • The extension list is a semicolon delimited list • The only wildcard used is a ? (which means any one character, could be empty) • The extension begins with a period "." If the problem continues, contact customer support.
Message	343 Antivirus Warning: Out of Memory! Cannot continue parsing extension list, restoring default of Scan All Files
Explanation	There may be a memory leak.
User Action	Reboot the appliance and contact Customer Support.
Message	343 Antivirus Warning: Parsing extension. Restoring default of Scan All Files
Explanation	There may be a memory leak.
User Action	Restart your machine and call tech support.
Message	343 Antivirus Warning: Scanner required by rule but not configured
Explanation	The proxy is configured to scan files, but does not have an IP address for the antivirus scan server.
User Action	Check the server setting in antivirus scan server IP address.
Message	343 Antivirus Warning: Failed to open control socket 343 Antivirus Warning: Failed to connect to the antivirus scan server due to <*error #*>

Table B-6 Antivirus scanning messages

Explanation	There was an error opening the connection or initializing the connection to the antivirus scan server.
User Action	Check to make sure the antivirus scan server is running and listening. Also make sure the configuration variables are correct. The proxy will block the connection if configured to do so.
Message	343 Antivirus Warning: Buffer overflow on file name 343 Antivirus Warning: Buffer overflow on headers
Explanation	The filename or header given to the antivirus scan server interface (for a particular transaction) is too long and will cause a buffer overflow. This could be an attack. The proxy will block the connection if configured to do so.
Message	343 Antivirus Warning: Failed send on antivirus scan server socket due to *<error #>*
Explanation	The firewall could not send data to the antivirus scan server.
User Action	Make sure the antivirus scan server is up and running and accepting connections.
Message	343 Antivirus Warning: Out of Memory! 343 Antivirus Warning: Error checking extension!
Explanation	An error occurred while checking a file against the file extension list
User Action	No user action is needed. Since this may signal an attack, the file is automatically scanned.
Message	343 Antivirus Warning: select failed due to *<error #>* 343 Antivirus Warning: recv failed due to *<error #>*
Explanation	There was an error receiving data from the antivirus scan server, which caused the proxy to drop the connection.

Table B-6 Antivirus scanning messages

User Action	Check to make sure the antivirus scan server is up and running.
Message	343 Antivirus Warning: The antivirus scan server detected <*threat*> and <*action*> Where *threat* can be one of the following: • one or more viruses/trojans/worms • a policy violation • both an infection and a policy violation and *action* can be one of the following: • took no action • repaired the file • deleted or rejected the file If the threat listed in the message is a virus/trojan/worm, an additional message is displayed: Threat description is <*threat name*> Where *threat name* is the name of the threat (or the name of the first threat if more than one threat is detected).
Explanation	Messages of this sort are sent if an attack is detected.
User Action	Take appropriate action to address the attack.
Message	343 Antivirus Warning: Error extracting headers from data received from antivirus scan server 343 Antivirus Warning: Aborting receive to prevent buffer overflow
Explanation	There was an error processing the antivirus scan server response. The antivirus scan server interface will return an error to the proxy and the proxy will drop the connection.
User Action	Contact customer support.

Appendix C

Licenses

The LINUX operating system used in Symantec Gateway Security appliance is covered by the GNU General Public License. The firewall software is covered by the Symantec license included with the license serial number.

To view licensed and enabled features

1. Select the icon of the connected appliance in the left pane.
2. Expand the **Base Components** folder.
3. Click the **System Features** icon.

   The licensed features and their status (Enable or Disable) is displayed in the right pane. If you want to change the status of a feature double click on the feature to display the feature's properties page.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1 This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program," below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification.") Each licensee is addressed as "you."

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2 You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3 You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be

licensed as a whole at no charge to all third parties under the terms of this License.

If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4 You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above, provided that you also do one of the following:

Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for

noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5 You may not copy, modify, sublicense or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated, so long as such parties remain in full compliance.

6 You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7 Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8 If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your

obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9 If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10 The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11 If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make

exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1 BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING, THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2 IN NO EVENT, UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING, WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

SYMANTEC APPLIANCE LICENSE AND WARRANTY AGREEMENT

SYMANTEC CORPORATION AND/OR ITS SUBSIDIARIES ("SYMANTEC") IS WILLING TO LICENSE THE SOFTWARE INCLUDED WITH THE APPLIANCE YOU HAVE PURCHASED TO YOU AS AN INDIVIDUAL, THE COMPANY, OR THE LEGAL ENTITY THAT WILL BE UTILIZING THE SOFTWARE (REFERENCED BELOW AS "YOU OR YOUR") AND TO PROVIDE WARRANTIES ON THE APPLIANCE ONLY ON THE CONDITION THAT YOU ACCEPT ALL OF THE TERMS OF THIS LICENSE AND WARRANTY AGREEMENT. READ THE TERMS AND CONDITIONS OF THIS LICENSE AND WARRANTY AGREEMENT CAREFULLY BEFORE USING THE APPLIANCE. THIS IS A LEGAL AND ENFORCEABLE CONTRACT BETWEEN YOU AND SYMANTEC. BY OPENING THIS PACKAGE, BREAKING THE SEAL, CLICKING ON THE "AGREE" OR "YES" BUTTON OR OTHERWISE INDICATING ASSENT ELECTRONICALLY, REQUESTING A LICENSE KEY OR USING THE SOFTWARE AND THE APPLIANCE, YOU AGREE TO THE TERMS AND CONDITIONS OF THIS AGREEMENT. IF YOU DO NOT AGREE TO THESE TERMS AND CONDITIONS, CLICK ON THE "I DO NOT AGREE" OR "NO" BUTTON IF APPLICABLE AND DO NOT USE THE SOFTWARE AND THE APPLIANCE.

1. Software License:

Except for the software, if any, described in the Excluded Software section at the end of this agreement (the ("Excluded Software"), the software (the "Software") which accompanies the appliance you have purchased (the "Appliance") is the property of Symantec or its licensors and is protected by copyright law. While Symantec continues to own the Software, you will have certain rights to use the Software after your acceptance of this license. This license governs any releases, revisions, or enhancements to the Software that the Licensor may furnish to you as well as the copy of the Software provided to you on a CD-ROM or other media in connection with the Appliance (the "Restore Software"). Except as may be modified by a Symantec license certificate, license coupon, or license key (each a "License Module") which accompanies, precedes, or follows this license, your rights and obligations with respect to the use of this Software are as follows:

You may:

A use the Software solely as part of the Appliance for no more than the number of users as have been licensed to you by Symantec under a License Module;

B use the Restore Software solely to restore the Appliance to its original factory functionality in the event the Software preloaded on the Appliance is corrupted or becomes unusable;

C make copies of the printed documentation which accompanies the Appliance as necessary to support your authorized use of the Appliance; and

D after written notice to Symantec, in connection with a transfer of the Appliance, transfer the Software on a permanent basis to another person or entity, provided that you retain no copies of the Software, Symantec consents to the transfer and the transferee agrees in writing to the terms of this agreement.

You may not:

A sublicense, rent or lease any portion of the Software; reverse engineer, decompile, disassemble, modify, translate, make any attempt to discover the source code of the Software, or create derivative works from the Software;

B use the Restore Software for any purpose other than to restore the Appliance to the original factory functionality;

C use, if you received the Software distributed on an Appliance containing multiple Symantec products, any Symantec software on the Appliance for which you have not received a permission in a License Module; or

D use the Software in any manner not authorized by this license.

2. Content Updates:

Certain Symantec software products utilize content that is updated from time to time (antivirus products utilize updated virus definitions; content filtering products utilize updated URL lists; firewall products utilize updated firewall rules; vulnerability assessment products utilize updated vulnerability data, etc.; collectively, these are referred to as "Content Updates"). You may obtain Content Updates for any period for which you have purchased a subscription for Content Updates for the product or otherwise separately acquired the right to obtain Content Updates. This license does not otherwise permit you to obtain and use Content Updates.

3. Limited Warranty:

Symantec warrants that the media on which the Restore Software is distributed will be free from defects for a period of thirty (30) days from the date of purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, replace any defective media returned to

Symantec within the warranty period or refund the money you paid for the Restore Software.

Symantec warrants that the Software will perform on the Appliance in substantial compliance with the written documentation accompanying the Appliance for a period of thirty (30) days from the date of purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Software returned to Symantec within the warranty period or refund the money you paid for the Appliance.

Symantec warrants that the hardware component of the Appliance (the "Hardware") shall be free from defects in material and workmanship under normal use and service and substantially conform to the written documentation accompanying the Appliance for a period of three hundred sixty-five (365) days from the date of purchase of the Appliance. Your sole remedy in the event of a breach of this warranty will be that Symantec will, at its option, repair or replace any defective Hardware returned to Symantec within the warranty period or refund the money you paid for the Appliance.

The warranties contained in this agreement will not apply to any Software or Hardware which:

A has been altered, supplemented, upgraded or modified in any way; or

B has been repaired except by Symantec or its designee.

Additionally, the warranties contained in this agreement do not apply to repair or replacement caused or necessitated by: (i) events occurring after risk of loss passes to You such as loss or damage during shipment; (ii) acts of God including without limitation natural acts such as fire, flood, wind earthquake, lightning or similar disaster; (iii) improper use, environment, installation or electrical supply, improper maintenance, or any other misuse, abuse or mishandling; (iv) governmental actions or inactions; (v) strikes or work stoppages; (vi) Your failure to follow applicable use or operations instructions or manuals; or (vii) such other events outside Symantec's reasonable control.

Upon discovery of any failure of the Hardware, or component thereof, to conform to the applicable warranty during the applicable warranty period, You are required to contact us within ten (10) days after such failure and seek a return material authorization ("RMA") number. Symantec will promptly issue the requested RMA as long as we determine that you meet the conditions for warranty service. The allegedly defective Appliance, or component thereof, shall be returned to Symantec, securely and properly packaged, freight and insurance prepaid, with the RMA number prominently displayed on the exterior of the shipment packaging and with the Appliance. Symantec will have no obligation to accept any Appliance which is returned without an RMA number.

Upon completion of repair or if Symantec decides, in accordance with the warranty, to replace a defective Appliance, Symantec will return such repaired or replacement Appliance to You, freight and insurance prepaid. In the event that Symantec, in its sole discretion, determines that it is unable to replace or repair the Hardware, Symantec will refund to You the F.O.B. price paid by You for the defective Appliance. Defective Appliances returned to Symantec will become the property of Symantec.

Symantec does not warrant that the Appliance will meet your requirements or that operation of the Appliance will be uninterrupted or that the Appliance will be error-free.

THE ABOVE WARRANTIES ARE EXCLUSIVE AND IN LIEU OF ALL OTHER WARRANTIES, WHETHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF INTELLECTUAL PROPERTY RIGHTS. THIS WARRANTY GIVES YOU SPECIFIC LEGAL RIGHTS. YOU MAY HAVE OTHER RIGHTS, WHICH VARY FROM STATE TO STATE.

4. Disclaimer of Damages:

SOME STATES AND COUNTRIES, INCLUDING MEMBER COUNTRIES OF THE EUROPEAN ECONOMIC AREA, DO NOT ALLOW THE LIMITATION OR EXCLUSION OF LIABILITY FOR INCIDENTAL OR CONSEQUENTIAL DAMAGES SO THE BELOW LIMITATION OR EXCLUSION MAY NOT APPLY TO YOU.

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW AND REGARDLESS OF WHETHER ANY REMEDY SET FORTH HEREIN FAILS OF ITS ESSENTIAL PURPOSE, IN NO EVENT WILL SYMANTEC OR ITS LICENSORS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INDIRECT OR SIMILAR DAMAGES, INCLUDING ANY LOST PROFITS OR LOST DATA ARISING OUT OF THE USE OR INABILITY TO USE THE SOFTWARE EVEN IF SYMANTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

IN NO CASE SHALL SYMANTEC'S OR ITS LICENSORS' LIABILITY EXCEED THE PURCHASE PRICE FOR THE APPLIANCE. The disclaimers and limitations set forth above will apply regardless of whether you accept the Software or the Appliance.

5. U.S. Government Restricted Rights:

RESTRICTED RIGHTS LEGEND. All Symantec products and documentation are commercial in nature. The software and software documentation are "Commercial Items", as that term is defined in 48 C.F.R. section 2.101, consisting of "Commercial Computer Software" and "Commercial Computer Software Documentation", as such terms are defined in 48 C.F.R. section 252.227-7014(a)(5) and 48 C.F.R. section 252.227-7014(a)(1), and used in 48 C.F.R. section 12.212 and 48 C.F.R. section 227.7202, as applicable. Consistent with 48 C.F.R. section 12.212, 48 C.F.R. section 252.227-7015, 48 C.F.R. section 227.7202 through 227.7202-4, 48 C.F.R. section 52.227-14, and other relevant sections of the Code of Federal Regulations, as applicable, Symantec's computer software and computer software documentation are licensed to United States Government end users with only those rights as granted to all other end users, according to the terms and conditions contained in this license agreement. Manufacturer is Symantec Corporation, 20330 Stevens Creek Blvd., Cupertino, CA 95014.

6. Export Regulation:

You agree to comply strictly with all applicable export control laws, including the US Export Administration Act and its associated regulations and acknowledge Your responsibility to obtain licenses as required to export, re-export or import the Appliance. Export or re-export of the Appliance to Cuba, North Korea, Iran, Iraq, Libya, Syria or Sudan is prohibited.

7. General:

If You are located in North America or Latin America, this Agreement will be governed by the laws of the State of California, United States of America. Otherwise, this Agreement will be governed by the laws of England. This Agreement and any related License Module is the entire agreement between You and Symantec relating to the Appliance and: (i) supersedes all prior or contemporaneous oral or written communications, proposals and representations with respect to its subject matter; and (ii) prevails over any conflicting or additional terms of any quote, order, acknowledgment or similar communications between the parties. This Agreement may only be modified by a License Module or by a written document which has been signed by both You and Symantec. This Agreement shall terminate upon Your breach of any term contained herein and You shall cease use of and destroy all copies of the Software and shall return the Appliance to Symantec. The disclaimers of warranties and damages and limitations on liability shall survive termination. Should you have any questions concerning this Agreement, or if you desire to contact Symantec for any reason, please write: (i) Symantec Customer Service, 175 W. Broadway,

Eugene, OR 97401, USA, or (ii) Symantec Customer Service Center, PO BOX 5689, Dublin 15, Ireland.

8. Excluded Software:

The Excluded Software consists of the open source code software known as Linux included with the Appliance. All Excluded Software is licensed under the GNU General Public License, Version 2, June 1991, a copy of which is included with the user documentation for the Appliance. The license entitles You to receive a copy of the source code for Linux only upon request at a nominal charge. If you are interested in obtaining a copy of such source code, please contact Symantec Customer Service at one of the above addresses for further information.

Appendix D

Serial Port Cable

Serial 9-Pin Cable Specifications

Use a cable the meets the following specifications to connect to the serial port of your appliance.

Table D-1 Serial 9-Pin Cable Connections

DB-9	Direction	Description
1	<	DCD (Data Carrier Detect)
2	<	RX (Receive Data)
3	>	TX (Transmit Data)
4	>	DTR (Data Terminal Ready)
5	...	GND (Signal Ground)
6	<	DSR (Data Set Ready)
7	>	RTS (Request To Send)
8	<	CTS (Clear to Send)
9	<	RI (Ring Indicator)

Index

A

Adding SRMCs 127
Address
    configuring during first system boot 35
    statements
        private entries for DNS 104
    transforms 8
Alerts
    viewing for IDS 142
Alias 107
    defining in host file 106
Antivirus scanning
    configuring 165
        proxy services 173
        scan server 168
    enabling in a rule 183
    local 166
    mail filter options 186
    messages 255
    on the Gateway Security Appliance 165
    overview 10
    remote 166
Asymmetric routing 241
Attack signature
    update using LiveUpdate 139
    using IDS attack signature 139

B

Back panel features
    model 5110 24
    models 5200/5300 26
Backup files 122
Battery 243
Blacklist notification 150
Blacklistd daemon
    configuring 152
Bloodhound 163

C

Change log command
    executing from SRMC 127
Client program notification 152
Cluster
    configuring VIPs 236
    creating for hardware HA/LB or file propagation 222
    creating for software HA/LB 215
    preparation 215
    verification 224
    Wizard
        deleting 214
        modifying 225
        using 214
Component list 15
Configuration
    antivirus scanning 165
    enabling antivirus scanning in a rule 183
    establishing mail policies for antivirus scanning 186
    files
        backing up from SRMC 122
        propagating 230
        restoring from SRMC 124
    gated option for IDS signatures 138
    IDS signatures for detection 137
    network worksheets 36
    proxy services for antivirus scanning 173
    Quickstart wizard 64
    reports 8
    Setup wizard 56
    SMTP wizard 70
Connectivity

to Gateway Security Appliance 54
verifying 108
Content
profiles
HTTP restrictions 209
restrictions 207
Content filtering 11
Content profiles 202
Custom services
configuring 8

D

Date and time
changing 118
Default
routes
configuring using Setup wizard 101
configuring using SRMC 101
Deleting
Executive Summary report 146
Denial of Service Attacks 8
Display
system information 42
DNS
configuring proxy 104
private file address statements 104
split-level 104
Documentation
supplied 16
Domain Name 58

E

Electric shock 244
Enable/disable
IDS 134

F

Factory reset 43
File
extensions
allowing 207
propagation 222
Filter signatures
by attack severity 137
by attack type 135
by operating system 136
FireProof 214
Firewall software patches
applying from SRMC 126
Flat network 100
Front panel
features
models 5200/5300 32
using locked key pad 129
FTP
configuring for antivirus scanning 174

G

Gated signature 138
GNU general public license 262

H

HA/LB
cluster properties 229
creating clusters 215, 222
deleting clusters 228
implementation 232
overview 12
verifying clusters 224
VIPs 236
Heartbeat network
description 240
High Availability and Load Balancing
see HA/LB
Host ID
see System ID 41
Host IP address
for SRMC 39
hosts.pub file 107
defining alias 106
HTTP
configuring for antivirus scanning 174
ratings
allowing extensions and URLs 207
URL patterns 210

I

IDS
enabling and disabling 134
identifying signatures to detect 137
informational messages 247
LiveUpdate 139
marking signatures gated or not gated 138
monitoring 133
notifications 147
refreshing the view in the IDS Alerts Viewer 144
reports
Configuration Report 145
Executive Summary 145
running LiveUpdate on demand 141, 142
scheduling LiveUpdate 140
signatures
configuring for detection 137
filtering by attack severity 137
filtering by attack type 135
filtering by operating system 136
marking gated or not gated 138
viewing additional information 139
viewing in the Signature Configuration window 134
updating attack signatures using LiveUpdate 139
viewing alerts 142
Incident node 240
Informational messages 247
Initial setup procedure 38
Installation
connecting
power cord 25, 27
to network 25, 27
powering on
model 5110 26
models 5200/5300 28
rack mount appliance 22
SRMC 48, 49
Uninterruptible Power Supply (UPS) connection 28
Intrusion Detection System
see IDS
IP address
configuring during initial setup 38
configuring virtual IP addresses for clusters 236

K

Keypad
using locked 129, 130

L

LEDs. See Status indicators.
License
GNU general public 262
Symantec appliance license and warranty agreement 267
License Key 58
obtaining 44, 119
Lithium battery 243
LiveUpdate 164
antivirus 171
disabling the scheduler 142
IDS 139, 140, 141, 142
running on demand 141, 171
scheduling 140, 171
Load balancing
network resources 232
Local antivirus scanning 166
Locked keypad
using 130
Log files
managing 127
Log messages
antivirus 255
IDS 247
Login
remote 128

M

Mail
notification 153
setup 64

Management Information Base (MIB) 157
Managing
    Gateway security functions 12
    log files 127
MIME types 211
Monitoring
    Gateway security functions 12
    mode 42

N

Netmask
    configuring during initial setup 38
Network
    address information 35
    configuration 35
    configuration worksheets 36
    connections
        model 5110 25
        models 5200/5300 27
    flat 100
    interfaces 59
    resources
        load balancing 232
    routed 100
    setup 43
    status indicators 32
Non-gated signature 138
Norton AntiVirus Extension (NAVEX) technology 164
Notifications
    Blacklist 150
    Client Program 152
    IDS 147
    Mail 153
    Page 155
    SNMP V1 158
    SNMP V2 159
NTFS 49

P

Page notification
    alphanumeric 156
    numeric 156
Password
    entering for SRMC initial setup 39
    managing using SRMC 116
    root 40
    Root and Secure Remote 116
    Security Gateway Appliance 55
    SRL 40
Patches
    applying 126
Ping command
    using 102, 108
Power
    applying for model 5110 26
    applying for models 5200/5300 28
    cord installation
        model 5110 25
        models 5200/5300 27
    switch 27
Preferred node 240
Private DNS entries
    configuring using SRMC 104
Profiles
    WebNOT 204
Protocols
    configuring custom services 8
Proxies
    antivirus 174
    DNS 104
Proxy services
    configuring for antivirus scanning 173
        FTP 174
        HTTP 174
        SMTP 178

Q

Quickstart wizard 64

R

Radware FireProof 224
Ratings profile
    creating 202
    customizing 206
    Net Ratings 202

searching capabilities 205
Rear view
power switch 27
Refreshing
IDS alerts in the viewer 144
Remote antivirus scanning 166
Remote login 128
Reports
IDS
Configuration Report 145
Executive Summary 145
Reset 43
Restart system
from SRMC 121
Restore Files
from SRMC 124
Root
password 40, 116
Routable addresses 8
Routed network 100
Routes
configuring default
using SRMC 101
Rules
antivirus 183
ratings profile 204

S

S2S Tunnel wizard 77
Safety
electric shock 244
equipment rack 244
Lithium battery 243
Scan server
antivirus 162
Scanning
antivirus 161
Scheduling
LiveUpdate to update IDS
attack signatures 140
Secure
Remote Login
password 116
Remote login 128
Tunnel wizards 79, 95
Setup
procedure
initial 38
wizard 56
Shutdown 43
Signatures
configuration window 134
filtering
by attack severity 137
by attack type 135
by operating system 136
SMTP wizard 70
SNMP Notifications
about 157
SNMP V1 158
SNMP V2 159
Software patches
applying to the firewall 126
Split-level DNS 104
SRL
client 128
password 40
SRMC
adding SRMCs 127
applying software patches to firewall 126
backing up configuration files 122
changing
date and time 118
license key 120
log command 127
system settings 117
configuring private DNS entries 104
filtering content 202
host IP Address 39
installing 48, 49
LiveUpdate
running on demand 171
scheduling 171
overview
password 39, 55
managing 116

root 116
Quickstart wizard 64
restarting system 121
restoring configuration files 124
root password 40
Secure Remote Login (SRL) 116
Setup wizard 56
SMTP wizard 70
system shutdown 121
Static routes
setting 100
Status indicators
100 M 30, 32
active connection 32
Col 30, 32
Disk 30, 32
hard disk drive 32
Link 30, 32
Temp 30, 32
traffic 32
Transmit/Receive 30, 32
Web activity 32
Sticky node 240
Striker technology 164
Symantec Gateway Security Models
5110 13
5200 14
5300 14
Symantec Raptor Management Console
see SRMC
Symantec warranty 267
Symmetric routing 241
System
ID 41
information 42
menu
factory reset 43
network setup 43
shutdown 43
system ID 43
UPS setup 43
messages at setup 28
name 58
restarting 121
settings
changing 117
shutdown
from SRMC 121

T

TCP/IP addresses
address transforms 8
Temperature 30, 32
Tera Term Pro 128
tgz file 126
Time and date
changing 118

U

Uninterruptible Power Supply (UPS) connection
models 5200/5300 28
Updating
IDS attack signatures using LiveUpdate 139
using Live Update 139
UPS setup 43
URL
blocking 202
ratings profile 202
restricting 207
wildcard character 209
User documentation 16

V

Verifying
clusters 224
connectivity 108
Viewing
Executive Summary report 146
IDS
alerts 142
signatures in the Signature Configuration window 134
VIPs
configuring addresses 236

Virus
detection 163
updating definitions 171

W

Warranty 267
Web setup 64
WebNOT 202
WebNOT Ratings Service 202
Wizards
cluster 214
S2S tunnel 77
setup 56
tunnels 79, 95
Worksheets
network configuration 36